A mes parents.

A ma famille.

A mes amis.

Oussama

Remercîments

Avant tout je remercie DIEU tout puissant car sans DIEU rein de tout ça n'aura lieu.

Je tiens à remercier tout d'abord mes parents pour leur soutient et leurs encouragements durant toutes mes années d'études. Je tiens à remercier aussi mon encadreur MR BELABED Amine pour son grand aide, ses conseils professionnels est son soutient moral, pour la liberté d'action qu'il m'a laissée et les orientations qu'il m'a fournies. Cela m'a permis de recadrer mon travail, en allant toujours vers l'avant. Je remercie également Mr Smahi M.I ,Mr Merzoug M et Mr Benmouna .Y D'avoir accepter de faire partie du jury. J'ai passé un peu plus de cinq années au sein de la faculté des sciences, ll y a eu des jours heureux et d'autres moins. Mais je tiens à remercier mes professeurs, ainsi que tous mes collègues et mes amis(es). Sans oublier Monsieur Habibes pour son soutient moral, en lui souhaitant de guérir le plus tôt possible.

Tables des matières

Introduction général

Contexte

Le monde d'aujourd'hui est d'une complexité croissante, en effet, le nombre d'habitants de notre planète augmente quotidiennement, et les gens se tournent de plus en plus vers les nouvelle technologies de l'information et de communication, pour gagner leur vie ou simplement se faire des amis et rester en contact avec eux .

L'accroissement de l'utilisation des nouvelles technologies d'informations et de communication exigent une sécurisation efficace qui permettra de garantir à la fois un maximum de confidentialité et un minimum d'échec.

Au début de l'utilisation des nouvelles technologies d'information et de communication, le niveau de sécurité était très bas qui a engendré des abus fréquents sur la vie privée, fautes de la naïveté des internautes, et les outils de sécurisation mis en place par ces nouvelles technologies, en particulier les réseaux sociaux. Par contre, de nos jours ,et grâce aux recherches faites par les chercheurs dans le domaines de la sécurisation ,ont trouvé de nouveaux outils pour faciliter notre utilisation des NTIC avec sécurité .

Problématique

Notre travail tourne au tour de la protection de la vie privée des utilisateurs des réseaux sociaux. Notre objectif est de mettre en place un outil qui permet de mieux gérer la confidentialité au sein d'un réseau social. Pour cela nous avons proposé un outil visuel qui permet à un utilisateur de voir la visibilité de ces informations de profil selon le point de vue de ces amis. Notre outil offre une manière souple de contrôler, de gérer et de modifier les informations personnelles.

Contribution

Pour atteindre ce but nous avons proposé un mini réseau social qui permet La création de liens d'amitiés, l'outil proposé est une partie intégrante de ce réseau.

Plan du mémoire

Le présent manuscrit est présenté selon trois chapitres, décrits comme suit : dans le premier chapitre nous allons introduire les notions clés concernant les réseaux sociaux à savoir leur l'histoire, leurs bases mathématiques et sociales, ainsi que leurs fonctionnements.

Le deuxième chapitre est consacré à la vie privée des utilisateurs dans les réseaux sociaux, Ce chapitre présente quelques atteintes sur la vie privée ainsi que quelques mécanismes de protection

Le troisième chapitre est consacré à une description de notre mini réseau social, et les détails de fonctionnement de notre outil d'amélioration de la confidentialité.

Enfin, une conclusion générale qui résume notre travail et introduit quelques perspectives.

Chapitre 1 : Introduction aux réseaux sociaux

I. Introduction

L'avènement des nouvelles technologies de communication et d'information ont modifié le web à jamais parmi les plus importants d'entre eux : le réseau social qu' on peut le définir comme des services Web qui permettent aux individus de crée un profil public dans un système borné, construire une liste d'autres membres avec lesquels ils partagent une connexion, et visualiser et de parcourir la liste de leurs connexions et celles faites par d'autres au sein du système. La nature et la nomenclature de ces connexions peuvent varier d'un réseau à l'autre.[1]Ce qui rend le réseau social unique c'est qu'il ne permet pas seulement aux individus de rencontrer des étrangers, mais plutôt il leur permettent aussi de définir et de rendre visible leurs réseaux sociaux. Cela peut entraîner des connexions entre les individus qui autrement ne seraient pas faites. Sur la plupart des réseaux sociaux de grande taille, les participants ne sont pas nécessairement à la recherche d'une rencontre de nouvelles personnes, mais plutôt l'envie de communiquer avec des personnes qui font déjà partie de leur réseau social étendu.

II.L'histoire des sites de réseaux sociaux

Le premier site de réseau social reconnaissable a était lancé en 1997 sous le nom SixDegrees.il permettait aux utilisateurs de créer des profils, la liste de leurs amis et, à partir de 1998, de surfer sur les listes d'amis. Chacun de ces éléments existait avant SixDegrees, Les Profils existaient sur la plupart des grands sites de rencontre et de nombreux sites communautaires. Les listes des amis étaient prises en charge pas AIM et ICQ, bien que ces amis ne sont pas visibles par les autres. Classmates.com permettait aux gens de s'affilier à leur école secondaire ou un collège et surfer sur le réseau pour d'autres qui ont également affilié, mais les utilisateurs ne pouvaient pas créer des profils ou des listes d'amis.

Des années plus tard SixDegrees a été le premier à combiner tous ces fonctionnalités. Alors que SixDegrees attiraient des millions d'utilisateurs, mais il a échoué à devenir une entreprise durable et, en 2000, le service fermera.

Alors que les gens commençaient juste de se familiariser avec Internet, la plupart n'avaient pas de réseaux étendus d'amis qui étaient en ligne. Ceux qui l'ont adopté se sont plaints qu'il y avait peu à faire après avoir accepté les demandes d'amis, et la plupart des utilisateurs ne se sont pas intéressés à rencontrer des étrangers. De 1997 à 2001, un certain nombre d'outils de communauté a commencé à soutenir diverses combinaisons de profils et amis publiquement articulés. AsianAvenue, BlackPlanet et MiGente permettaient aux utilisateurs de créer des espaces personnels, professionnels et leurs utilisateurs pourraient identifier des amis sur leurs profils personnels sans demander l'approbation pour ces connexions .De même, peu de temps après son lancement en 1999.une nouvelle vague de RS a commencé quand Ryze.com a été lancé en 2001 pour aider les gens à tirer parti de leurs réseaux d'affaires. Ryze a ouvert le chemin à de nombreux RS comme Friendster, MySpace et Facebook, trois réseaux sociaux clés qui ont façonné le paysage des affaires, de la culture et de la recherche.

II-1Friendster

Friendster a été lancé en 2002 comme un complément social à Ryze. Il a été conçu pour rivaliser avec Match.com,un site de rencontres en ligne rentable.Friendster se concentrait sur la création d' un lieu de rencontre entre les amis.il a connu un regain parmi les trois groupes de pionniers qui ont façonné les sites-blogueurs, les participants de l'Homme festival des arts de combustion, et les hommes gais (boyd, 2004) et a grandi à 300.000 utilisateurs à travers le bouche à oreille.[1]

Comme la popularité de Friendster a bondi, le site a rencontré des difficultés techniques et sociales. Les Serveurs et bases de données de Friendster étaient mal équipés pour gérer sa croissance rapide, et le site échouait régulièrement, c'est ce qui a conduit à sa fermeture

II-2MySpace

Alors que MySpace a été lancé avec l'esprit de faire la découverte de nouveaux musiciens et de rapprocher les fans de leurs stars, cette relation symbiotique aida MySpace à s'étendre. La dynamique des musiciens-et-fans a été mutuellement bénéfique: les musiciens voulaient être capables de communiquer avec les fans, tandis

que les fans souhaitaient l'attention de leurs groupes préférés et utiliser les connexions amies pour signaler l'identité et l'appartenance. En outre, MySpace se démarque en ajoutant régulièrement des fonctionnalités basées sur la demande des utilisateurs et en permettant aux utilisateurs de personnaliser leurs pages. Cette "fonctionnalité" a émergé parce que MySpace ne peut pas restreindre les utilisateurs d'ajouter dans les formulaires HTML qui encadraient leurs profils, un code de culture copier / coller vu le jour sur le web pour aider les utilisateurs à générer des milieux uniques MySpace et mises en page (Perkel, sous presse).Les adolescents ont commencé a rejoindre MySpace en masse à partir de 2004. Contrairement aux utilisateurs plus âgés, la plupart des adolescents n'ont jamais été sur Friendster-certains ont rejoint parce qu'ils voulaient communiquer avec leurs groupes préférés, d'autres ont été introduits sur le site par des membres âgés de la famille. Comme les adolescents ont commencé à signer, ils encourageaient leurs amis à les rejoindre. Plutôt que de rejeter les utilisateurs mineurs, MySpace a changé sa politique pour permettre son utilisation à des mineurs. Comme le site a grandi, trois populations distinctes ont commencé à se former: musiciens, adolescents, foule urbaine post-collège sociale[1].

II-3Facebook

Le nom de ce réseau social phénomène fait référence aux albums photo créés au cours de la scolarité des étudiants d'Harvard. Son créateur, Mark Zuckerberg, a eu l'idée de ce réseau social pour permettre aux étudiants de cette prestigieuse université d'échanger des sujets de cours. Il a étendu son ingénieux concept à d'autres universités américaines pour s'ouvrir au monde entier en 2006. Aujourd'hui Facebook compte plus de 750 millions d'utilisateurs dans le monde et plus de 25 millions en France. Ouvrir un compte Facebook est d'une simplicité remarquable et d'une rapidité inouïe. La force de Facebook et sa popularité grandissante résident surtout dans le fait que cette plate-forme est totalement gratuite [2].(voir figure I-1)

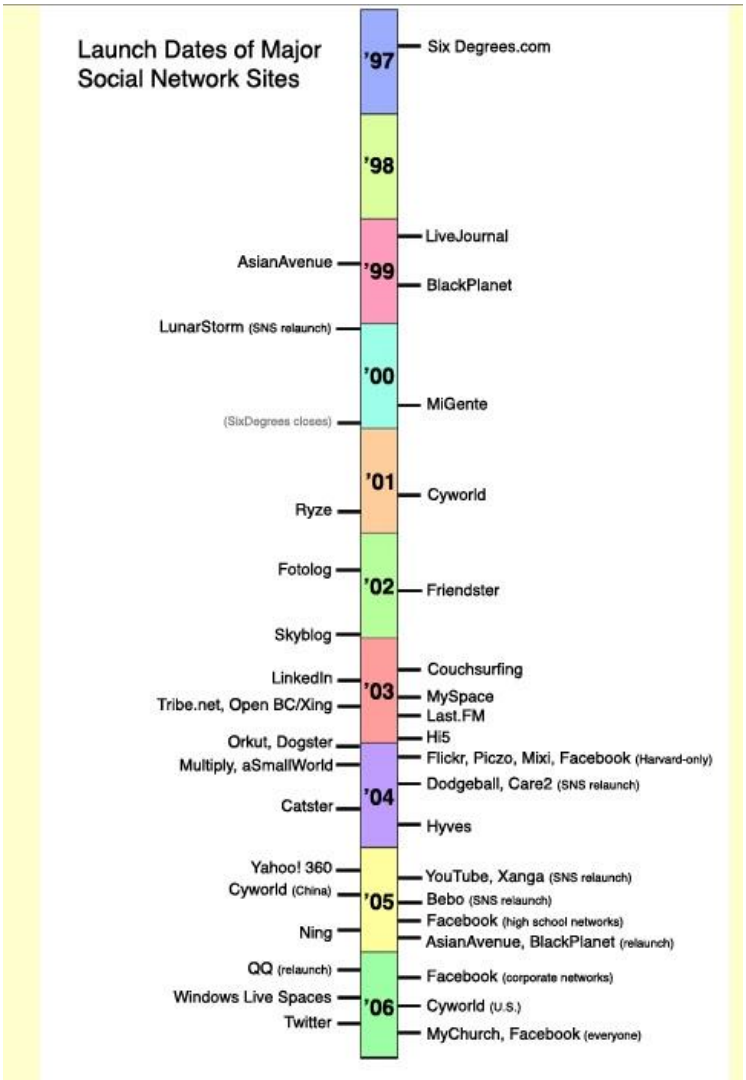


Figure I 1 la chronologie des lancements des réseaux sociaux [1]

III. Le fonctionnent d'un réseau social

D'une façon général les RS fonctionnent de la même manière, ils mettent en œuvre un large éventail de caractéristiques techniques, leur structure est constituée de profils visibles qui affichent une liste d'amis qui sont également des membres du système, ces profils sont des pages uniques. Après avoir rejoint un RS en créant son profil, le nouveau membre est invité à remplir un formulaire contenant une série de questions. (voir figure I-2)

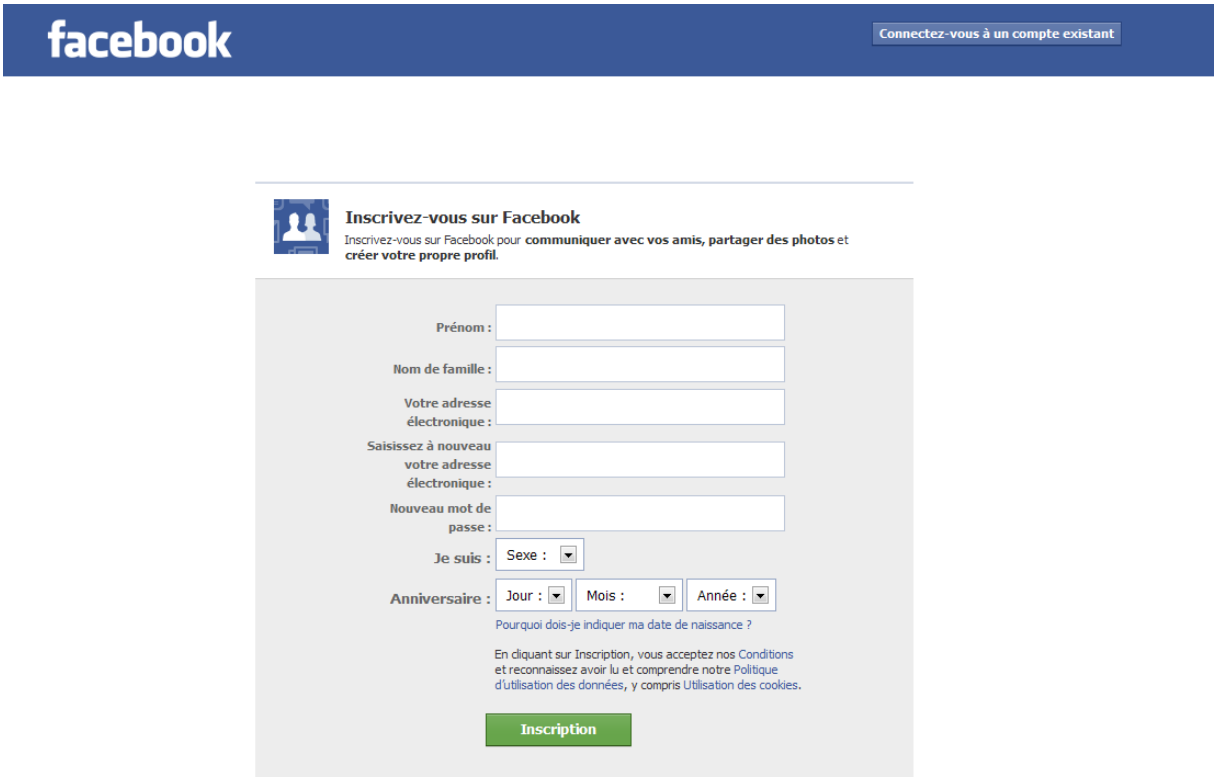


Figure I-2 exemple de création d'un profil [4]

Le profil est généré à l'aide de réponses à ces questions, qui comprennent généralement des descripteurs tels que l'âge, le lieu de naissance, les intérêts et une "About Me" section. La majorité des RS encouragent aussi les membres à télécharger une photo de profil. Certains sites permettent aux membres d'améliorer leur profil en ajoutant du contenu multimédia ou de modifier leur profil regard et sensation. D'autres, tels que Facebook, permettent aux membres d'ajouter des modules ("Applications") qui améliorent leurs profils.(voir figure I-3)

Figure I-3 personnaliser un profil [4]

La visibilité d'un profil varie selon les sites et selon les choix des membres. Par défaut, les profils sur Friendster et Tribe.net sont analysés par les moteurs de recherche, ce qui les rend visibles par toute personne, indépendamment de si oui ou non le spectateur a un compte. Alternativement, LinkedIn contrôle quel spectateur peut voir, si il ou elle a un compte payant. Des sites tels que MySpace permettent aux utilisateurs de choisir s'ils veulent que leur profil soit public ou «Amis uniquement».

Facebook prend une approche différente, par défaut, les membres qui font partie du même «réseau» peut voir les profils des uns comme les autres, sauf si le propriétaire du profil a décidé de refuser la permission à ceux du réseau.

Les variations structurales autour de la visibilité et l'accès sont un des principaux moyens de différencier les réseaux sociaux les uns des autres .Après avoir rejoint un site de réseau social, les membres sont invités à identifier d'autres dans le système avec lequel ils entretiennent une relation. L'étiquette de ces relations varie en fonction des conditions du RS incluent «Amis», «Contacts» et «ventilateurs». La plupart des RS

exigent une confirmation bidirectionnelle pour l'amitié, mais d'autres pas l'affichage public des connexions est une composante essentielle du RS. La liste d'amis comporte des liens vers le profil de chaque ami, ce qui permet aux téléspectateurs de parcourir le réseau par le biais des listes d'amis. Sur la plupart des sites, la liste des amis est visible à quiconque est autorisé à afficher le profil, mais il ya des exceptions. Par exemple, certains membres de MySpace ont piraté leurs profils pour masquer l'affichage des amis, et LinkedIn permet aux membres de se retirer de l'affichage de leur réseau. La plupart des réseaux sociaux fournissent également la fonction de commentaire qui permet aux membres de laisser des messages sur les profils de leurs amis. Au-delà des profils des amis, des commentaires et des messages privés, les RS varient considérablement dans leurs caractéristiques. Certains se basent sur le partage de photos ou vidéos selon les capacités de partage, d'autres ont intégré dans les blogs et la technologie de messagerie instantanée. Il ya certains qui prennent également en charge les interactions limitées mobiles (par exemple, Facebook, MySpace et Cyworld). Bien des RS sont souvent conçus pour être largement accessibles, beaucoup pour attirer des populations homogènes d'abord, il n'est donc pas rare de trouver des groupes utilisant les réseaux sociaux séparés par la nationalité, l'âge, le niveau d'éducation, ou d'autres facteurs que la société en général, même si ce n'était pas l'intention des concepteurs.

IV. Les bases sociales des SRS

IV-1 les six degrés de séparation

Les Six degrés de séparation est une idée qui repose sur le fait que deux personnes sur cette planète peut être connecté via un nombre moyen de six étapes [3].(voire figure I-4)

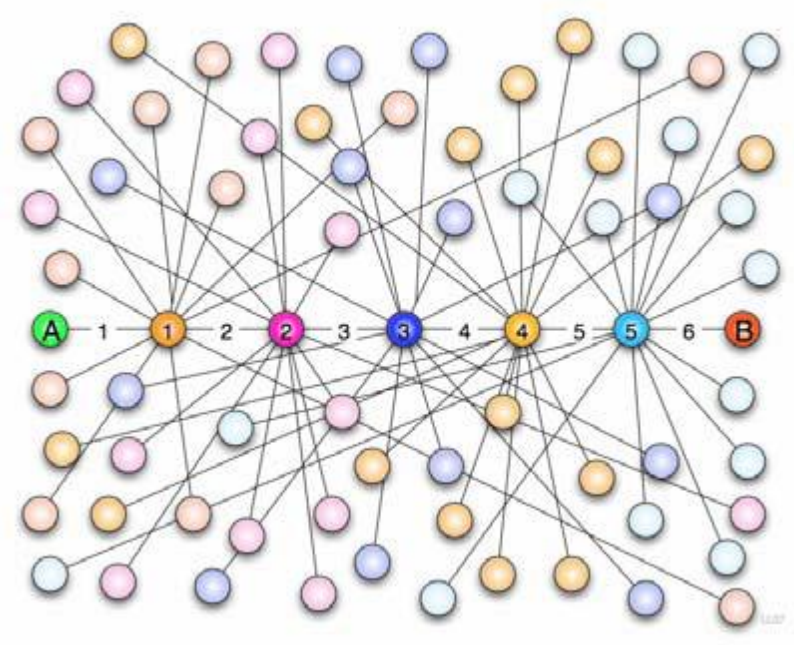


Figure I-4 Exemple illustratif des six degrés de séparation [3]

a-Règle de 150 :

Cette règle repose sur le principe de L'anthropologue et biologiste de l'évolution, le Britannique Robin Dunbar établit à 148 «la limite cognitive du nombre de personnes avec lesquels un individu peut avoir des relations stables». Concrètement, chaque individu ne peut avoir un réseau social de plus de 150 membres[2] .

b-La loi de Reed :

La loi de Reed est le résultat des recherche de David Reed ,cette loi affirme qu' un membre est relié au réseau entier comme à un tout, mais également à beaucoup de sous-ensembles significatifs du tout. Ces sous-ensembles ajoutent de la valeur à l'individu comme au réseau lui-même. En incluant des sous-ensembles dans le calcul de la valeur du réseau, la valeur augmente plus rapidement qu'en se cantonnant à ne prendre en compte que les nœuds. Cette loi est particulièrement adaptée aux réseaux ou individus, communautés et groupes plus ou moins formels sont considérés [2].

V. La base mathématique des réseaux sociaux

La première représentation d'un réseau social était faite par Jacob Levy Moreno au début des années 1930, il avait pour objectif la visualisation graphique d'un réseau social.

Il a représenté les personnes par des points et une relation entre deux personnes par des flèches. Cette représentation est depuis désignée par le terme sociogramme, mais on parlait également de toiles en raison de leur aspect en toile d'araignée. Cette forme de visualisation, aussi peu innovante qu'elle puisse paraître de nos jours, fut un premier outil d'identification rapide des caractéristiques d'un réseau social. Cette représentation a attiré le regard des mathématiciens qui ont fait le rapprochement entre les représentations sociogrammes et la théorie des graphes au sens mathématique. Par la suite Le graphe est devenu la représentation adoptée par toutes les sciences impliquant l'analyse des réseaux sociaux. Nous vous présentons une liste de quelques notions manipulées par la théorie des graphes pour les réseaux sociaux[5] :

- Le sommet :C'est l'unité de base d'un réseau, il en représente une ressource. Dans un réseau social on parle d'acteur. Le terme nœud est également utilisé pour désigner un sommet.

- L'arête : elle représente la connexion entre deux sommets. Il existe plusieurs types d'arête :

  · Une hyper-arête est une arête qui connecte deux ou plusieurs sommets.
  · Une arête est orientée si elle ne s'utilise que dans une seule direction.
  · Une arête non orientée est une arête qui s'utilise dans les deux directions.
  · Une arête est pondérée lorsqu'on lui attribue un poids.
  · Une arête est étiquetée lorsqu'on lui attribue un label.

- Le graphe : il se définit par un ensemble de sommets et un ensemble d'arêtes, les types des graphes se définissent par rapport à leurs arêtes :

  · Un hypergraphe est défini par un ensemble de sommets et un ensemble d'hyper arête.
  · Un graphe orienté est un graphe avec des arêtes orientées.
  · Un graphe pondéré est un graphe avec des arêtes pondérées.
  · Un graphe étiqueté est un graphe avec des arêtes étiquetées.
  · Un graphe multipartites st un graphe avec des sommets de types différents.

- Le degré :il se définit comme le nombre des arêtes adjacentes a un sommet

- Un chemin : le chemin représente la séquence d'arêtes qui relie deux sommets

VI. Conclusion

Nous avons introduits dans ce chapitre la notion de réseau social et les étapes clefs dans son évolution, nous avons vu qu'il se base sur des théories mathématiques et des théories sociales, et que la majorité des réseaux sociaux fonctionnent de la même façon. dans le chapitre suivant on va introduire la notion de danger qui peut représenter la faiblesse de ces réseau, parmi ces dangers : vols d'identités, fraudes… y sont bel et bien présents, ce qui nous amène à penser à la protection de la vie privée, la question que nous devons poser est : comment bien protéger nos renseignements ?

Chapitre2 : la vie privée dans les réseaux sociaux

I. Introduction

Il est difficile de définir avec exactitude Le droit au respect de la vie privée qui est un droit fondamental, c'est ce que nous allons voir tout le long de ce chapitre. Les interprétations du droit au respect de la vie privée dépendent depuis longtemps des technologies disponibles et avec l'arrivée web, qui a inévitablement remodelé ce que nous entendons par respect de la vie privée. Dans ce chapitre nous allons introduire la notion de la vie privée, les mécanismes de protection sur le web et sur les réseaux sociaux en particulier.

II.la définition de la vie privée

Le droit de la vie est profondément ancré chez les êtres humains, il est fondé sur la notion d'intégrité et de dignité personnelles. Toutefois, cela est aussi difficile à définir avec un degré convenu de précision.

Le droit de la vie privée englobe le droit à la liberté de pensée et de conscience, le droit d'être seul, le droit de contrôler son propre corps, le droit de protéger sa réputation, le droit à une vie familiale.

De plus, ces notions varient d'un contexte à un autre. En dépit de son ambigüité, il n'y a pas de définition de la vie privée qui soit universellement comprise de la même façon.

Dans le monde moderne, la vie privée comporte les questions relatives à l'identité d'une personne tel que son adresse, son lieu de travail et la façon dont les informations personnelles sont traitées et collectées peut être mises en vente pour les sociétés publicitaires [6].

III. Les atteintes sur la vie privée et principes de protections

L'atteinte à la vie privée se définie comme l'accès non autorisé à des renseignements personnels ou la collecte, l'utilisation ou la communication non autorisée de tels renseignements.

Cette activité est « non autorisée » lorsqu'elle contrevient aux lois applicables en matière de protection de la vie privée.

Certains des cas d'atteinte à la vie privée les plus fréquents se produisent lorsque des renseignements personnels sont volés, perdus ou communiqués par erreur. Une atteinte à la vie privée peut également découler d'une erreur de procédure ou d'une défaillance opérationnelle.

Pour prévenir des atteintes on peut suivre l'exemple des Principes de protection de la vie privée appliquée au sein des entreprises canadiennes, ces principes définissent le droit fondamental à la protection de la vie privée des personnes et les obligations des entreprises à cet égard [7].

Une personne est responsable des renseignements personnels sous votre garde ou confiés à une tierce partie aux fins de traitement.

Il faut Déterminer et documenter les fins auxquels des renseignements personnels sont recueillis avant leur collecte ou leur utilisation.

Les personnes doivent être informées de toute collecte, utilisation ou communication de renseignements personnels qui les concernent et y consentir. Toutefois, il existe certaines exceptions.

Il ne faut recueillir que les renseignements personnels nécessaires aux fins déterminées et procéder de façon honnête et licite.

Il ne faut pas utiliser ou communiquer les renseignements personnels qu'aux fins auxquelles ils ont été recueillis, à moins que la personne concernée ne donne son consentement. Ne gardez les renseignements personnels que le temps nécessaire.

Les renseignements personnels doivent être aussi exacts, complets et à jour que le requièrent les fins déterminées.

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

Il faut faire preuve de transparence concernant vos politiques et procédures visant à protéger les renseignements personnels. Faites en sorte que ces politiques et procédures soient compréhensibles et facilement accessibles. Les personnes ont le droit de savoir si vous possédez des renseignements personnels qui les concernent, et ont le droit d'y accéder. Elles pourraient aussi avoir le droit de les faire corriger.

Les personnes ont le droit de porter plainte à l'égard du non-respect des principes de protection de la vie privée.

IV. Les attaques sur la vie privée dans les réseaux sociaux

Dernièrement, face à l'avancé spectaculaire dans le domaine de la technologie de l'information et de la communication. La notion de la vie privée c'est vue adoptée à la nouvelle aire médiatique, elle est définie «le droit de vie privée et la revendication des individus, des groupes ou des institutions de décider eux-mêmes quand, comment et dans quelle mesure les informations les concernant sont communiquées à autrui,C'est le désir des individus de choisir librement dans quelles circonstances et dans quelle mesure ils livrent leur personne, leurs attitudes et leurs comportements à autrui»[6]. La forte popularité des réseaux sociaux a conduit à de nombreuses études relatives à la sécurité et aux aspects de protection de la vie privée, Dans cette partie nous allons étudier quelques exemples d'attaques relatives aux réseaux sociaux les plus populaires

IV-1 Le phishing (Hameçonnage)

Le phishing se définit comme un ensemble de techniques utilisées par les hackers pour réunir des informations personnelles d'internautes trop confiants. Cette technique consiste dans l'utilisation des pirates de sites web et courriels qui imitent ceux d'institutions financières, d'organismes gouvernementaux ou bien de grandes marques connues et dignes de confiance. Ces pirates arrivent souvent à convaincre les internautes à divulguer des informations privées liées à leurs banques telles que le nom d'utilisateur, le mot de passe, ou le numéro de carte de crédit [8].

Le bilan annuel du phishing-iniative.com, un site internet qui permet aux internautes de lutter contre le hameçonnage en soumettant les mails frauduleux qu'ils ont reçus, publié le 21 mars 2013, révèle que plus de 50 000 sites ou adresses ont été dénoncés par les Français, contre 30 000 en 2011. Après vérification, les analystes ont établi qu'en 2012, 30 000 de ces adresses étaient effectivement des plateformes crées dans le but de voler des données personnelles ou bancaires.

Il existe plusieurs variantes du phishing dont nous citons :

a- Le spear phishing :

Cette forme de phishing vise une organisation spécifique en cherchant des accès non autorisé à des données confidentielles.
Ces attaques ont pour but l'accès à des secrets commerciaux ou bien de mettre la main sur des renseignements militaires.

b- Le phishing vocal :

Il a beaucoup de similitudes avec au le phishing classique, mais au lieu de fournir un lien frauduleux pour que le client clique dessus, il donne un numéro de téléphone. Ce type d'arnaque utilise le plus souvent des fonctionnalités de téléphonie IP difficilement contrôlable par les gouvernements et à faible coût pour exploiter la confiance de l'utilisateur dans les services de téléphones fixes. Ce qui facilite l'accès aux informations personnelles et financières des internautes.

IV-2 Le vol d'identité

Le vol d'identité est le fait de voler l'identité d'une personne et se faire passer pour cette même personne dans le but d'accéder à ses ressources ou faire des transactions en son nom. Cela peut être pour différents buts : avoir un crédit, acheter des marchandises en son nom ou profiter de services réservés à la victime en utilisant ses documents personnels comme son passeport ou son assurance de santé.
Il y a plusieurs façons d'obtenir en ligne les informations personnelles des victimes [8].

IV-3 Les malwares :

Ce sont des logiciels malveillants installés à l'insu de la victime, conçus pour collecter des informations sensibles et pour obtenir un accès non autorisé aux systèmes informatiques. Il existe plusieurs types de malwares, dont les plus dangereux sont les Keylogging. Ce sont des logiciels malveillants qui interceptent les frappes de claviers faites par la victime sans qu'elle ne se rende compte. Ils peuvent intercepter les mots de passe, messages privés et n'importe quelles informations saisies par l'utilisateur.
Toutes ces informations sont ensuite envoyées aux fraudeurs qui les analysent et trient les données sensibles [8].

IV-4 Les attaques sur Facebook

Les informations sur la vie privée publiées sur Facebook peuvent être lues et utilisées par des personnes à qui elles n'étaient pas initialement destinées. Certaines entreprises utilisent Facebook pour collecter des informations sur leurs employés tandis que des recruteurs s'en servent pour leur sélection de candidats : « Les recruteurs appuyaient par fois un refus d'embauche sur des détails privés ainsi collectés ».Par ailleurs, certains parents se servent de Facebook pour surveiller la vie de leurs enfants De nombreuses ONG de défense des droits de l'homme et de la vie privée des personnes, comme l'Electronic Frontier Foundation ou Privacy International, s'inquiètent de cette nouvelle manière de récolter des informations sur les internautes et de les utiliser. Elles la considèrent comme d'autant plus pernicieuses qu'elles se mettent en œuvre avec la parfaite collaboration des utilisateurs de Facebook, qui n'ont pas nécessairement conscience des dangers d'une telle concentration d'informations entre les mains d'une entreprise privée, de leur vente à d'autres entreprises, ou de leur mise à disposition aux autorités fédérales américaines à leur demande.

Il semblerait également que les employés de Facebook puissent avoir accès aux pages de tous les utilisateurs du service. Fin novembre 2007, un réseau lancé par MoveOn a fait pression pour défendre la vie privée des utilisateurs du site, et a lancé une pétition en ligne. De nombreux groupes se sont créés sur Facebook pour dénoncer ce viol de la vie privée des utilisateurs du site.

V-5 Les attaques sur Myspace

Les personnes titulaires des comptes Myspace peuvent sélectionner les personnes pouvant accéder à leurs informations personnelles. En théorie, ce renforcement de sécurité destiné à rassurer les utilisateurs est efficace, et si les usurpateurs ne venaient pas de là où les utilisateurs les attendent? Après Facebook, c'est bien Myspace qui est accusé d'utiliser les données personnelles de ses utilisateurs. Le site les transmettrait notamment à des firmes publicitaires et donnerait même un accès direct à ces dernières aux informations personnelles des utilisateurs pouvant contenir leur nom, age, sexe, et même parfois leur adresse. Bien que la véracité de ces accusations n'a pas été vérifié.

V. Les systèmes de protection de la vie privée dans les réseaux sociaux

Nous allons introduire quelques systèmes de protection qui ont déjà prouvé leur efficacité

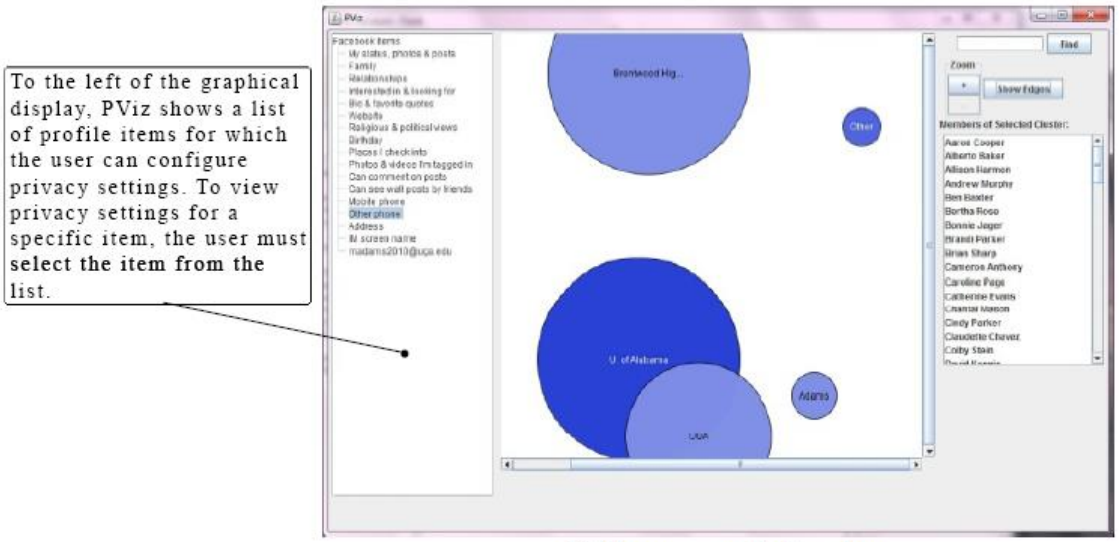
V-1 The PViz

PviZ système de protection de vie privée correspondant directement à la façon avec laquelle les modèles de groupes utilisateurs ainsi que les politiques de confidentialité sont appliqués à leurs réseaux. Il permet à l'utilisateur de comprendre la visibilité de son profil en fonction de la nature de ses groupes d'amis avec un niveau différent de granularité.

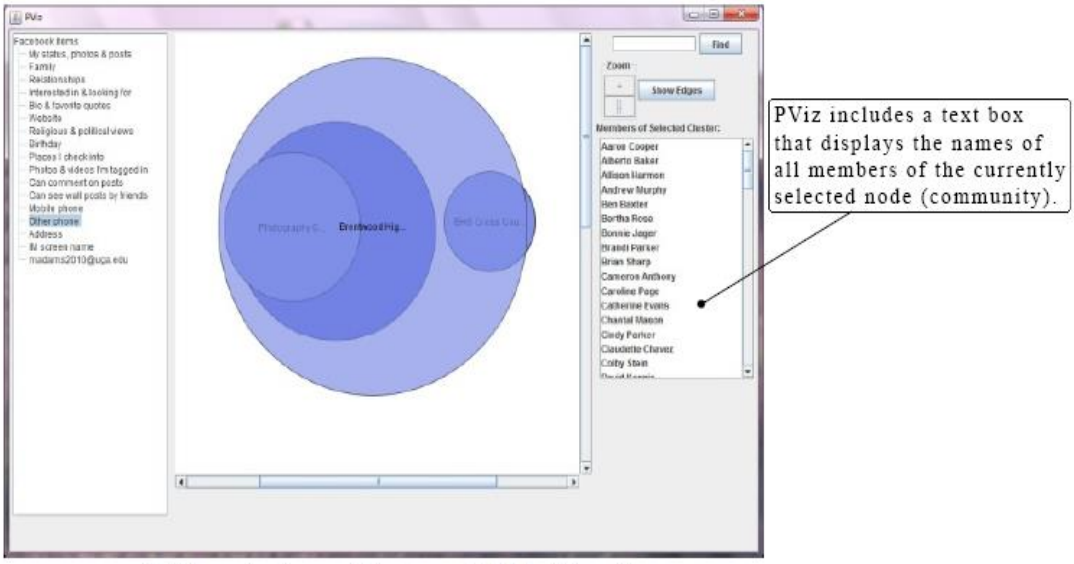
Le PViz est centré sur une interface graphique, qui montre le réseau social de l'utilisateur. Chaque nœud de l'affichage représente une sémantique significative d'un groupe d'amis de l'utilisateur ou un ami individuel [9].

Un prototype de PViz était mis dans le contexte de Facebook. Après que l'utilisateur se connecte à Facebook, PViz télécharge Toutes les données nécessaires à partir du compte de l'utilisateur. La Liste d'amis de l'utilisateur actuel, le graphique de réseau de voisinage (l' les amis de l'utilisateur courant et les connexions entre ces amis) .

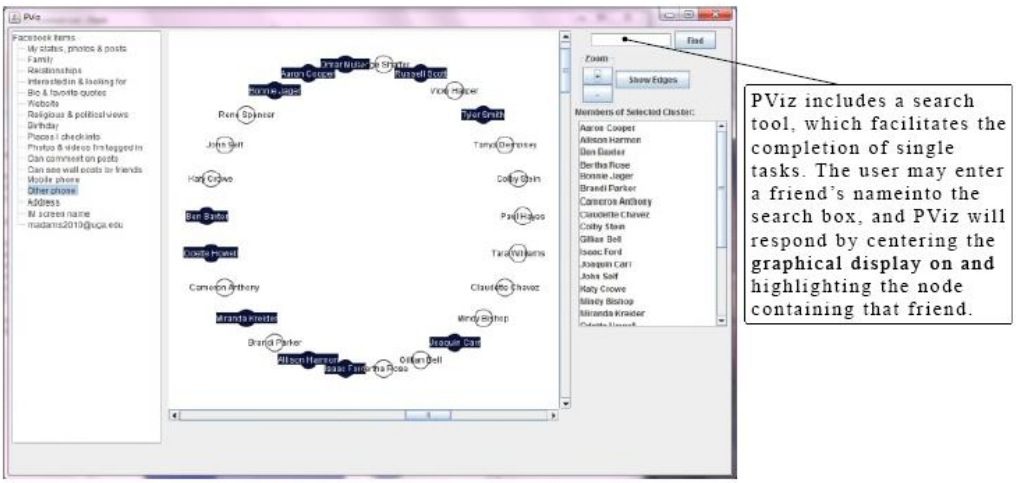
Le PViz utilise un outil de grattage écran pour télécharger et traiter les paramètres de confidentialité de l'utilisateur, la figure II-1 montre les déférentes étapes de l'implémentation du PViz ,ou il extrait une hiérarchie de communautés selon un processus récursif simple dans lequel le réseau est divisé en communautés fondées sur le maximum de modularité et de chaque communauté est traitée comme un autre réseau qui est à nouveau divisé. Cette opération est répétée jusqu'à ce qu'il n'y ait plus de partitionnement qui améliore la modularité. L'interface PViz est assez générale que d'autres algorithmes de détection de la communauté, ainsi que explicites groupements fournies par l'utilisateur, peuvent être facilement intégrés. Après que le réseau est divisé en communautés, PViz positions des nœuds sur l'écran en utilisant un Fruchterman Reingold(force-based.)



(a) Coarse granularity view



(b) Zooming in on “Brentwood High School”



(c) Fine granularity view

Figure II- 1 les déférentes étapes de l'implémentaiton du PViz[9]

V-2 The Privacy Wizard

C'est un Assistant de confidentialité qui a pour objectif de configurer automatiquement les paramètres de confidentialité de l'utilisateur. Pour ça, l'utilisateur fixe un ensemble de paramètres de confidentialité manuellement, et l'assistant utilise l'apprentissage machine (un classificateur) pour qu'il configure automatiquement le reste.

l'assistant sollicite un nombre limité de quantité d'entrée de l'utilisateur. L'utilisation de cette entrée, et d'autres informations déjà visibles pour l'utilisateur, l'assistant déduit un modèle décrivant la vie privée préférence personnelle de l'utilisateur pré-préférences VACY. Ce modèle est alors utilisé automatiquement pour les paramètres de confidentialité détaillés de l'utilisateur.il utilise un assistant d'échantillonnage, qui est basé sur un paradigme d'apprentissage actif.

Il utilise également un outil de visualisation, qui permet aux utilisateurs d'afficher et modifier le modèle qui en résulte[10].

Les déférentes étapes du fonctionnement de cet assistant est montré par la figure II-2

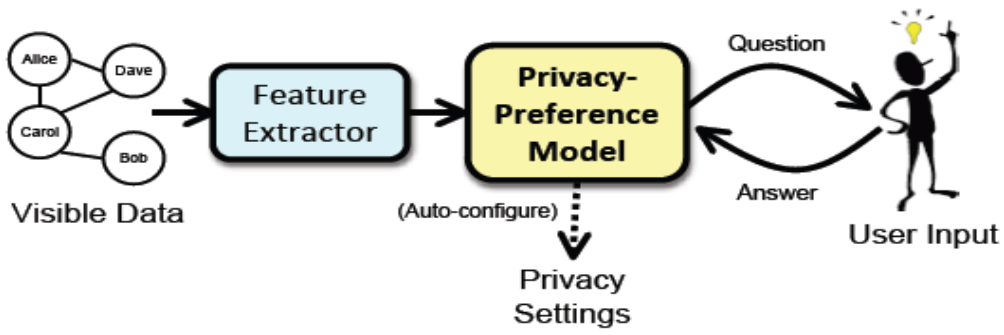


Figure II- 2 le fonctionnement du Privacy Wizard

V-3 SONARS (Social Networks-Based Algorithm for Social Recommender Systems)

Sonars, est un algorithme de recommandation contenu dans les systèmes de recommandation sociale. SONARS cible les utilisateurs en tant que membres des réseaux sociaux, ce qui suggère des éléments qui reflètent la tendance du réseau lui-même, basé sur sa structure et sur les relations d'influence entre les usagers [11].

VI. Conclusion

Dans ce chapitre nous avons introduit la notion de vie privée e les dangers qui peuvent l'atteindre sur le web et sur les réseaux sociaux, on a introduit quelques systèmes de protection

dans le dernier chapitre nous avons proposé une application qui permettra de mieux sécurisé son profile web

Chapitre3 : Conception et Implémentation

I. Introduction

Le but de ce chapitre est de présenter notre travail , qui consiste à concevoir un mécanisme qui permet d'améliorer la protection de la vie privée des utilisateurs dans les réseaux sociaux pour cela, nous allons voir les différentes étapes suivies durant la réalisation de notre application , nous commençons par présenter les différents diagrammes de conception (cas d'utilisation ,séquence, classe) suivie d' un exemple d'implémentation de notre mécanisme ainsi que les autres aspects essentiels du mini réseau social.

II .Conception de l'application

II -1 Diagrammes des Cas d'utilisations :

a- Le cas d'utilisation : authentification

L'Internaute a accès a une interface où il peut entrer son mot de passe et son nom utilisateur. Le système a accès à une base de données où il peut vérifier l'existence du mot de passe et du nom d'utilisateur (voir figure III-1) .

Figure III-1diagramme de cas d'authentification

b-Diagramme d'accès aux fonctionnalités du profil

Après l'authentification, l'internaute a accès à sa page d'accueil, cette page contient plusieurs liens, qui permettent à l'internaute de : modifier ces informations, voir ces messages, accéder à la liste des membres du réseau, et voir ses photos.(voir la figure III-2)

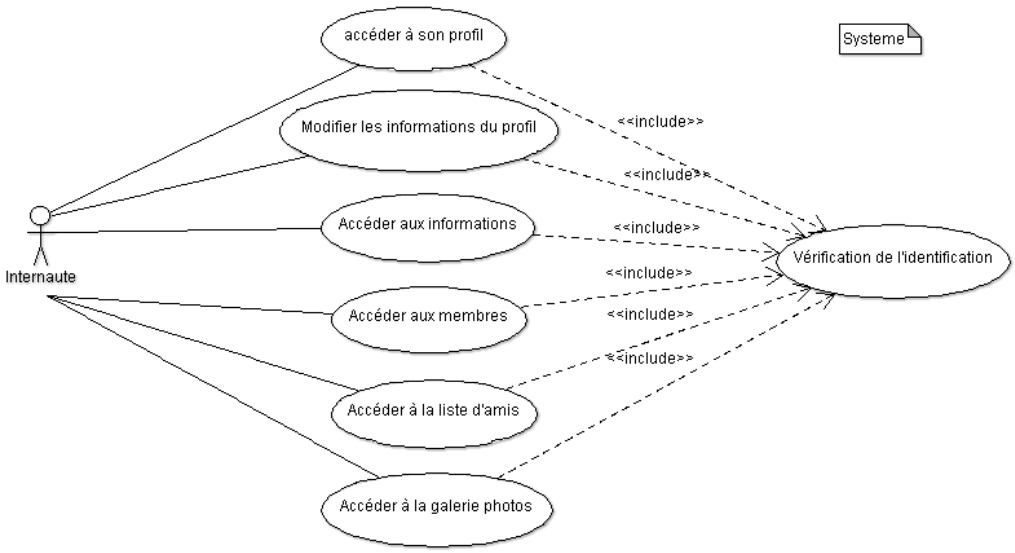


Figure III-2 diagramme de cas d'accès au profil

c-Diagramme du paramétrage de la vue profil

L'internaute a un accès à une interface système qui lui permet de modifier l'affichage de ces informations, le système enregistre les modifications dans sa base de données (voir figure III-3)

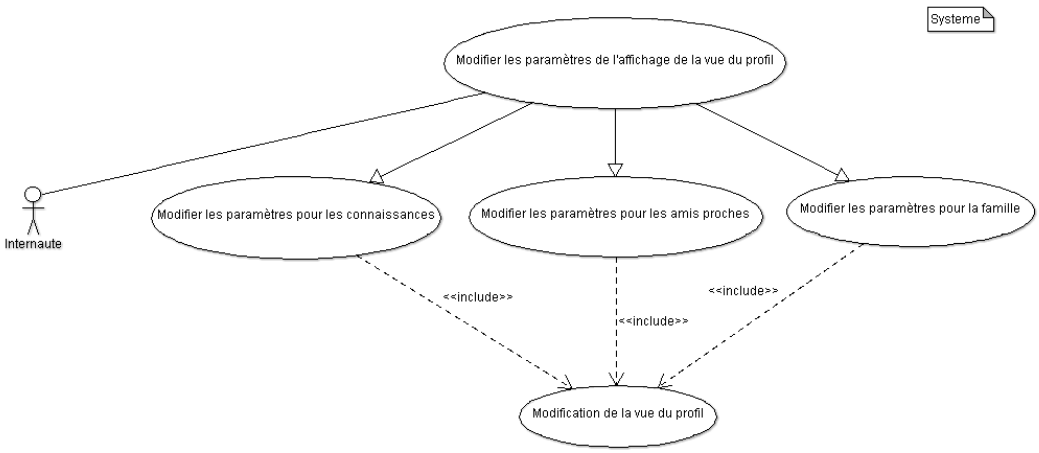


Figure III-3 diagramme de cas de paramétrage de la vue profil

d-Diagramme d'accès à un profil

L'internaute a accès a une interface systèmes qui lui permet de voir le profil d'ami ou de voir comment cet ami voit son profil (voir figure III-4)

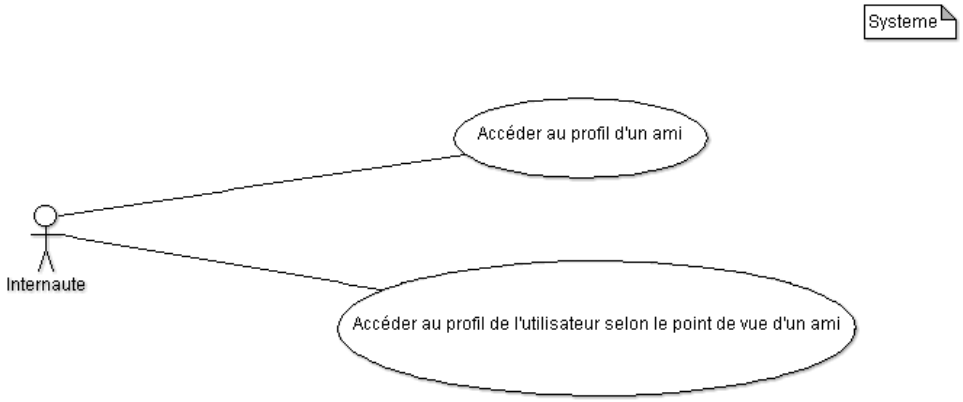


Figure III-4 diagramme de cas d'accès a un profil

II-2 Diagrammes des Séquences :

a-Diagramme de séquence de l'authentification

Comme elle le montre la figure III 6

- l'internaute entre son mot de passe et son nom d'utilisateur sur l'interface système
- L'interface système envoie les données récupérées au système d'authentification
- le système d'affichage a accès à la base de données où il vérifie leurs existences dans la table membres
- le système d'affichage renvoie les résultats de la recherche si les données existent, il donne à l'internaute l'accès à son profil
- si les données n'existent pas, les deux ou l'un d'eux retourne un message d'erreur

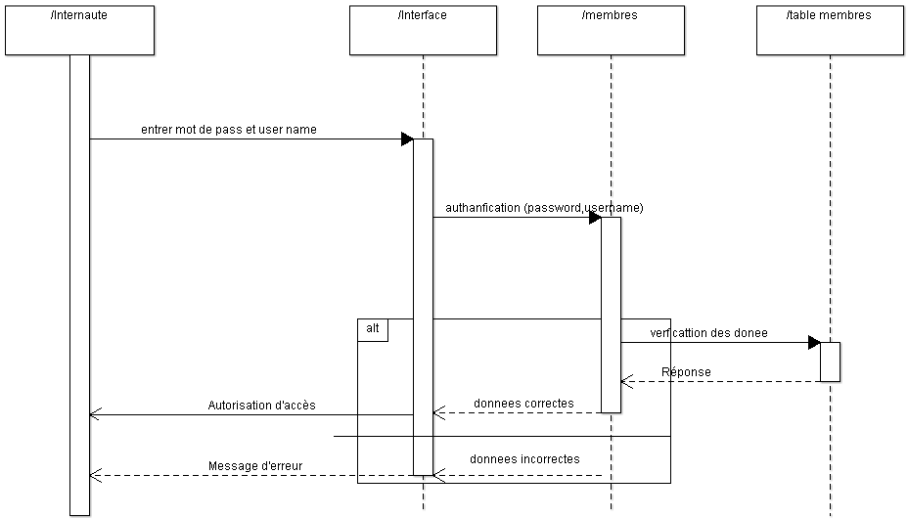


Figure III-5 diagramme de séquence de l'authentification

b- Diagramme de séquence du paramétrage de l'affichage

Dans la fonctionnalité de paramétrage on a trois alternatives (connaissances, amis proches, et famille) et ce paramétrage s'effectue de la même façon (voir figure III-7) :

- L'internaute entre les paramètres sur l'interface système
- L'interface système envoie les données au système d'affichage
- Le système d'affichage enregistre les nouveaux paramètres d'affichage sur la table d'affichage
- Le système d'affichage retourne à l'internaute un message : les modifications sont faites

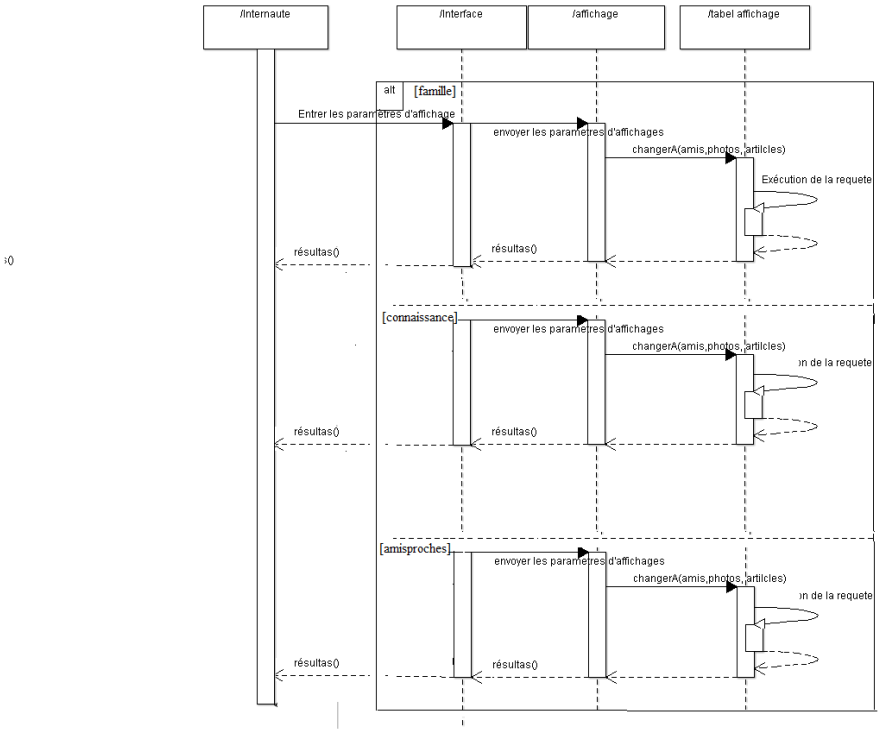


Figure III-6 diagramme de séquence du paramétrage de l'affichage

II-3 Digramme de classe :

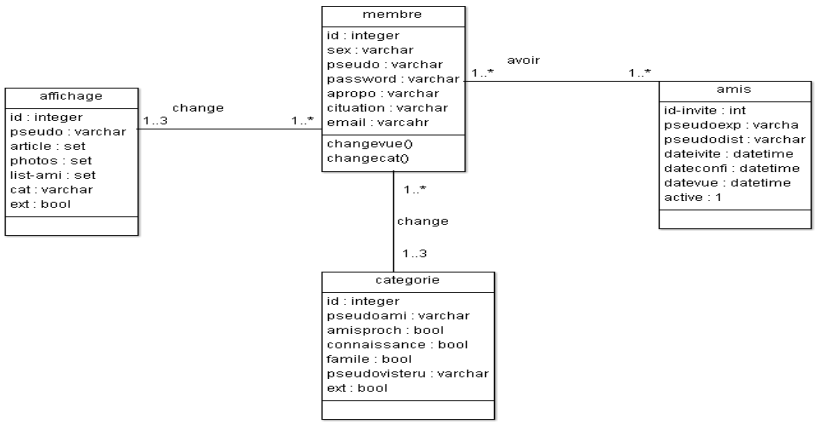


Figure III-7 diagramme de classe

III .Présentation du mécanisme :

Pour mieux protéger la confidentialité des utilisateurs dans un réseau social, nous avons proposé un mécanisme visuel qui permet à un utilisateur de voir comment son profil ainsi que ses informations sont visible par ses amis .Cet outil aide beaucoup l'utilisateur à paramétrer et à régler le niveau de confidentialité et de visibilité des ses informations. L'aspect visuel donne à l'utilisateur une vue très claire sur le niveau de protection de ses données par conséquent une très grand facilité de protection.

Pour bien expliquer le fonctionnement de notre mécanisme de protection on va prendre l'exemple d'un utilisateur « Oussama » qui envoie à l'utilisateur « amine » une demande d'amitié. Après l'acceptation « amine »va figurer dans la liste des amis de « Oussama »

(voir figure III-8)

Figure III-8 fenêtre de la liste des amis

Dans la page des amis , « Oussama »a deux possibilités la première permet d'accéder aux profils des amis en cliquant sur leurs noms ou sur leurs avatars (voir figure III-9)

Figure III-9 le profil d'ami

La deuxième possibilité montre le fonctionnent de notre mécanisme qui permet à « Oussama » de voir comment « amine » voit son profil. Le mécanisme offre à « Oussama » une fonctionnalité visuelle qui lui permet d'adapter la visibilité de ces

Informations personnelles vis-à-vis de sesamis.(voir figureIII-10)

Figure III-10 le profil de l'utilisateur selon le point de vue d'un ami

Ces adaptations sont possibles grâce à la fonctionnalité de La modification des paramètres de visibilité des informations de profil qui consiste à affecter chaque ami à une catégorie, notre outil offre trois catégories : connaissance, amis proches et famille .Chaque catégorie offre un niveau de visibilité prédéfinie, avec une possibilité de modifier les paramètres d'affichage de chaque niveau. Dans notre exemple « oussama » a mis « amine » dans la catégorie des amis proches, (voir figure III-11).

Figure III-11 la fonctionnalité de choix de catégories d'amis

Notre outil permet de modifier la visibilité de trois types d'information : les articles, les photos et la visibilité la liste d'amis. Dans notre exemple « Oussama » a modifié les paramètres d'affichage, il a choisi de montrer à ses amis proches toute sa liste d'amis, ces photos et ces articles (voir figure III-12). Le résultat de cette opération est présenté par la figure III-13

Figure III-12 la fonctionnalité de paramétrage de l'affichage

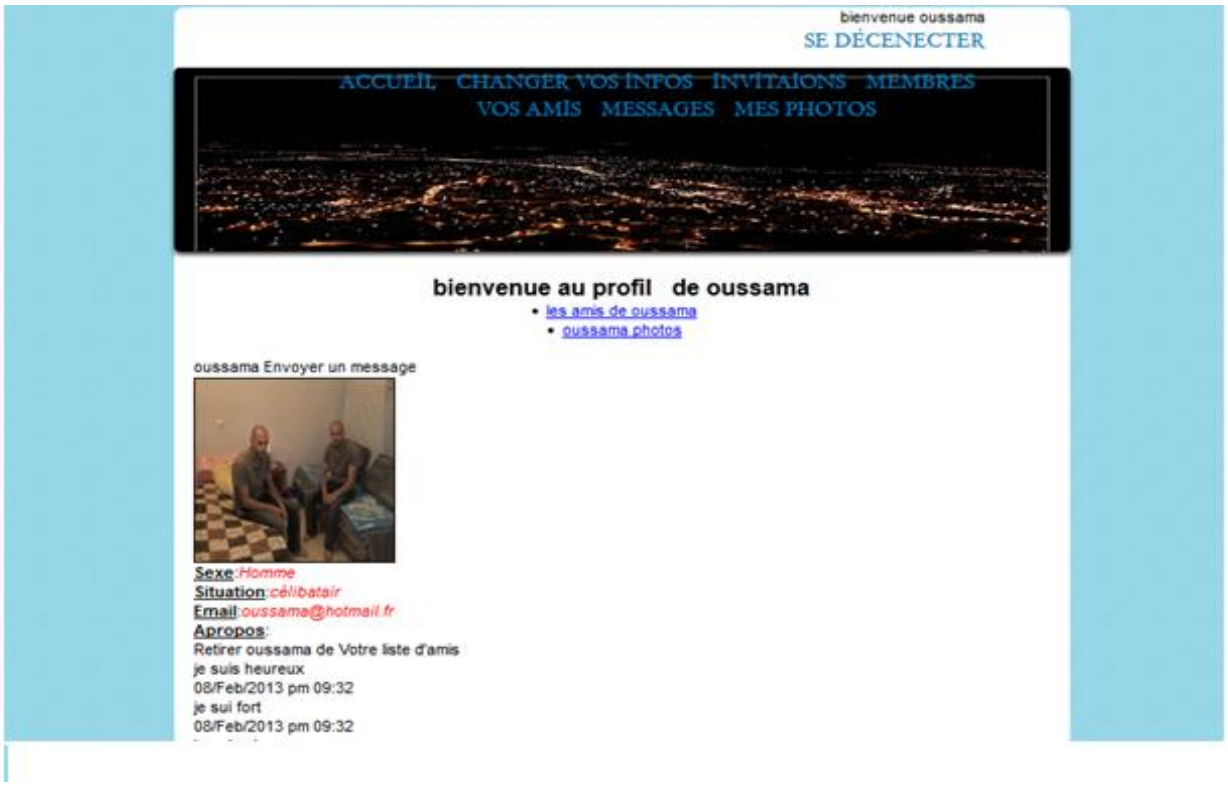


Figure III-13 la première possibilité d'affichage

Si « Oussama » choisit de ne pas montrer les articles, sa liste d'amis et ses photos il refait la même procédure précédente, le résultat d'une tel action est présenté dans la figure III-14

FigureIII-14deuxieme possibilité d'affichage

IV .Autres fonctionnalité du réseau

Dans cette partie nous présentons les aspects essentiels de notre réseau social :Comme tout réseau social , un utilisateur doit s'inscrire (voir figure III-15) si cette opération est déjà faite , l'utilisateur doit s'authentifie pour accéder à sa page de profil, il doit entrer son mot de passe et son nom d'utilisateur (voir figure III-16)

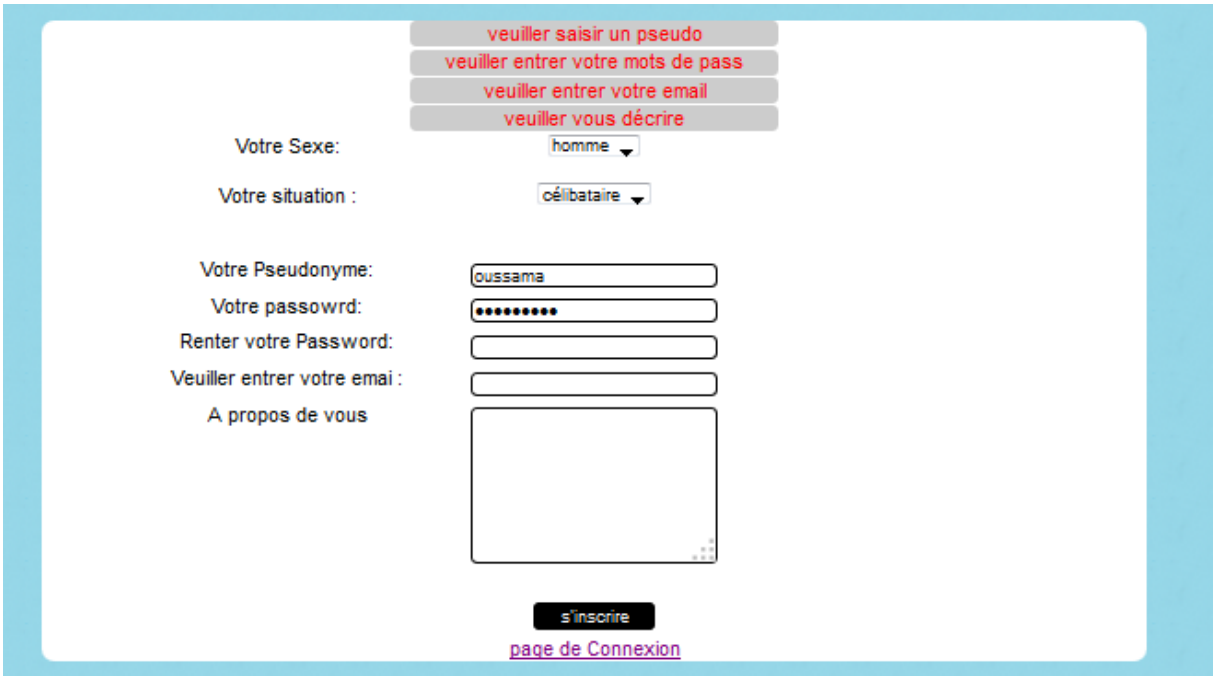


Figure III-15 fenêtre d'inscription

Figure III-16 page de connexion

Dans la page d'accueil (figure III-17) l'utilisateur peut accéder à autres pages, qui fournissent les fonctionnalités suivantes :

L'accès à la liste des membres inscrits dans notre réseau : dans cette page l'utilisateur peut voir tous les membres inscrits dans le réseau et il a la possibilité de voir leurs profils respectifs (voir figure III-18)

- L'accès la liste d'amis
- Le changement des informations du profil
- l'accès aux services de Messagerie (réception et envoi)
- L'accès à La galerie photos qui contient les photos personnelles de l'utilisateur

FigureIII-17 page d'accueil du profil

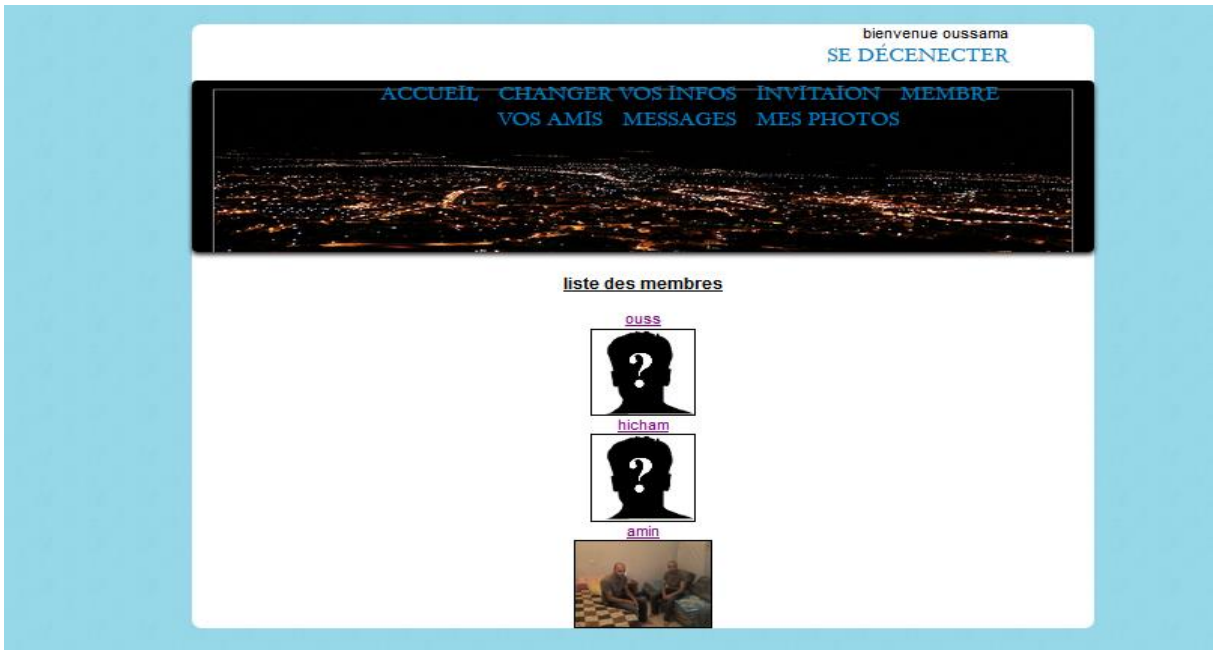
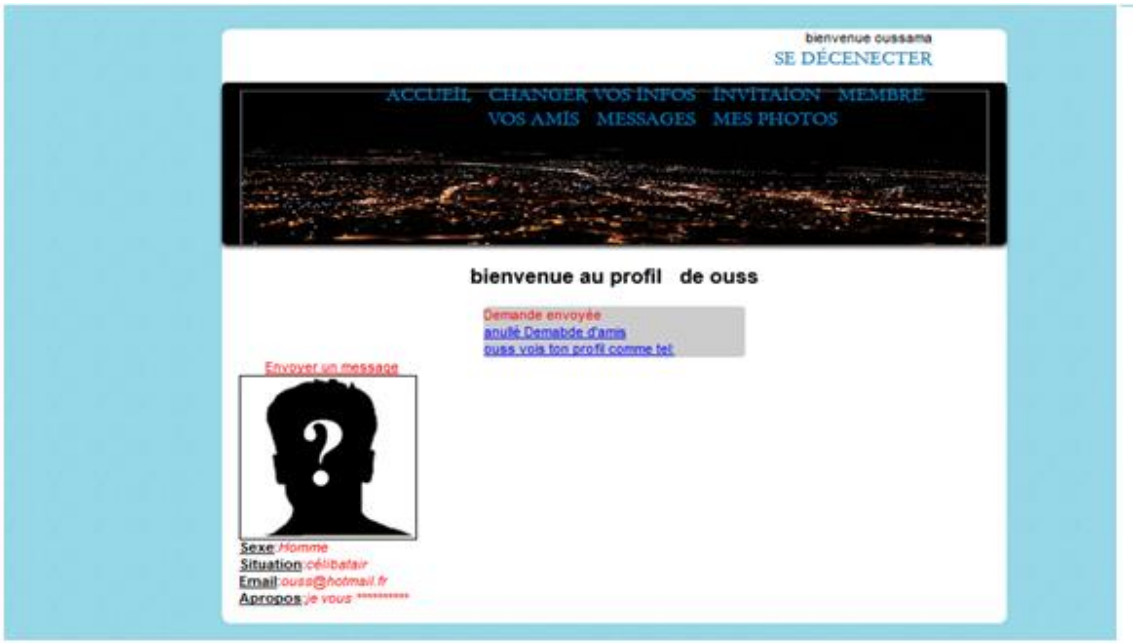


Figure III-18 pages des membres du réseau

Dans cette page et après que l'utilisateur choisit de voir le profil d'un membre du réseau, ou il a la possibilité de lui envoyer une demande d'amitié, et il a aussi accès aux informations de ce membre mises par défaut par le système. Ces informations sont :

la photo du profil, la situation personnelle, l'email, et la description du membre (voir figure III-19).



FigureIII-19 page de profil d'un membre

V .L'environnement de travail

Du fait que notre system est une application web nous avons utilisé le WampServer 2.2.1 qui est une plate-forme de développement Web sous Windows qui permet de développer des applications Web dynamiques dans un réseaux local .

Cette plateforme contient un serveur Apache2.2.11, du un moteur de scripts PHP 5.3.0 et le gestionnaire de base de données MySQL5.1.36. Il possède également PHPMyAdmin pour gérer plus facilement les bases de données,

Conclusion général

De nos jours le nombre d'utilisateurs des réseaux sociaux augmente, ce qui en résulte plus de quantité d'informations privées partagées. Ce qui fait apparaitre plusieurs problèmes liés à la protection de la vie privée tels que le vol d'identité, le hameçonnage… Tous ces problèmes ont emmené les chercheurs à se poser la question : Comment protéger les informations sensibles des utilisateurs des réseaux sociaux ?.

Plusieurs solutions ont été trouvées pour réduire ce risque que ce soit en proposant des modifications que les utilisateurs peuvent appliquer pour renforcer la protection de leurs comptes, ou bien en assistant les utilisateurs à faire ces modifications de façon automatique.

Dans le cadre de notre projet de fin d'étude le travail réalisé est basé sur l'étude conceptuelle qui est composée des (diagrammes des cas d'utilisations, des séquences et de classe) .

Comme dans tout logiciel, des améliorations restent toujours à apporter, faisons ainsi une liste non exhaustive des dites améliorations susceptibles d'être apporter ultérieurement à ce projet :

- Améliorer l'interface graphique de notre mini réseau social.
- Augmenter le nombre de paramètres d'affichages
- Spécifier d'autres catégories d'amis.

Les references

[1]danah m. boyd,Nicole B. Ellison,Social Network Sites: Definition, History, and Scholarship ,article University of California-Berkeley

[2]François Filliettaz, Marco Gregori,Un enjeu pour l'enseignement Comprendre les réseaux sociaux numériques,article,2011

[3] Wanqing Tu, Lei Zhang, ,Six Degrees of Separation in Online Society, article

[4] www.facebook.fr

[5] Romain Boulet,Théorie des graphes et étude de grands réseaux complexes. Applications à l'étude du droit de l'environnement,article, 2009

[6] toby mendel, andrew puddephatt, ben wagner, dixie hawtin et natalia torres,le respect de la vie privée sur l'internet et la liberté d'expression collection unesco sur la liberté de l'internet,article

[7] commissariat à la protection de la vie privée au canada , la protecition de la vie privée au sien de votre entreprise ,article

[8]. Eddine Gandouz,Un système communautaire pour la protection des usagers de Facebook,Juin, memoir,2012

[9] Alessandra Mazzia_ Kristen LeFevre_ and Eytan Adar, The PViz Comprehension Tool for Social Network Privacy Settings ,University of Michigan, Computer Science and Engineering, 2260 Hayward Ave. Ann Arbor, MI 48109,University of Michigan, School of Information, 105 South State St. Ann Arbor, MI 48109

[10] Lujun Fang and Kristen LeFevre ,Privacy Wizards for Social Networking Sites Electrical Engineering & Computer Science, University of Michigan 2260 Hayward Ave. Ann Arbor, MI 48109 USA

.[11] Carmagnola, F., F. Vernero, et al. (2009). SoNARS: A Social Networks-Based Algorithm for Social.Recommender Systems. Proceedings of the 17th International Conference on User Modeling, Adaptation, and Personalization: formerly UM and AH. Trento, Italy,Springer-Verlag: 223-234.

Liste des figures

Résumé

L’application présentée dans ce projet aborde l’amélioration de la protection de la vie privée sur les réseaux sociaux. La technique implémentée est basée sur la vue de son propre profil selon le point de vue des amis, cette vue permet de mieux adapter la sécurité dans son profil Les résultats obtenus sont assez satisfaisants, et encourageants les futurs travaux dans ce domaine de recherche.

MOTS CLES : réseaux sociaux, système de protection des réseaux sociaux, vie privée.