République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA-BEJAIA

Faculté des Sciences Exactes
Département d'Informatique

Mémoire

Présenté par

BENSIMESSAOUD Sihem

Pour l'obtention du diplôme de Magister

Filière : Informatique

Option : Cloud Computing

Thème

Préservation de la confidentialité des informations personnelles dans la publication des réseaux sociaux

29/09

Soutenu le : XX/XX/2016

Devant le Jury composé de :

Nom et Prénom	Grade		
M. TARI Abdelkamel	Professeur	Université de Bejaïa	Président
M. BADACHE Nadjib	Professeur	CERIST, Alger	Rapporteur
M. BOUKERRAM Abdallah	Professeur	Université de Bejaïa	Examinateur
Mme BENZAID Chafika	MCA	USTHB, Alger	Examinatrice
Mme BENMEZIANE Souad	CR	CERIST	Invitée

Année Universitaire : 2015/2016

Résumé

Aujourd'hui, de plus en plus les données du réseau social sont rendues publiquement disponibles à des fins d'analyse des données. Bien que cette analyse soit importante pour les chercheurs, il peut y avoir un risque de violation de la vie privée des utilisateurs constituant ce réseau social. Avec peu de connaissances locales sur les individus dans un réseau social, un adversaire peut réaliser différents types d'attaques. Parmi les informations que peut collecter un adversaire sur une victime cible, nous trouvons « le voisinage », c'est à dire, quels sont les voisins de la victime et comment ces voisins sont connectés. Cette information pourra ainsi aider l'adversaire à identifier la personne même si d'autres informations d'identification sont supprimées.

Dans notre travail, nous avons fait une étude détaillée de l'approche d'anonymisation proposée par Zhou et Pei [54] contre les attaques de voisinage et nous avons pu identifier quelques faiblesses concernant l'altération des propriétés structurelles du graphe anonymisé résultant. Ceci nous a conduit à proposer une nouvelle approche d'anonymisation des graphes sociaux à publier tout en maintenant l'utilité des données du réseau qui reflète les propriétés structurelles du graphe original notamment APL. La solution consiste à implémenter le modèle « k-voisinage » pour garantir que tout individu ne peut pas être identifié correctement dans le graphe social anonymisé avec une probabilité supérieure à 1/k, tel que pour chaque sommet appartenant au graphe, il existe au moins (k-1) autres sommets ayant des voisinages isomorphes.

Le but de l'approche proposée est d'une part de protéger les données publiées contre les attaques de voisinages et de préserver l'utilité du graphe social anonymisé d'autre part.