

Article	Année	Modèle de données	Nombre de parties	Primitives de sécurité	Evaluation expérimentale	Amélioration
Privacy-Preserving K-means Clustering over Vertically Partitioned Data [92]	2003	Vertical	n ($n > 2$)	-Permutation sécurisée [87]. -Le chiffrement homomorphe [84] -Le circuit d'évaluation de Yao [6]	Non	- Premier algorithme K-means sécurisé.
Privacy Preserving Clustering [97]	2005	Horizontal	2	-L'évaluation polynomiale Aveuglée [98]. -Le schéma de chiffrement homomorphe de Benaloh [82]	Oui	- Evaluation expérimentale. - Implémentation de deux protocoles différents.
Privacy –Preserving Distributed K-means Clustering over arbitrarily partitioned data [46]	2005	Arbitraire	2 (<i>extensible</i>)	- Les parts aléatoires [46] - Le produit scalaire sécurisé [88] - Le circuit d'évaluation de Yao [6]	Non	- Applicable à n'importe quel modèle de distribution de données. - Introduire l'idée du partitionnement arbitraire
Privacy preserving k-means clustering in multi-party environment. [93]	2007	- Horizontal - Vertical	n	-L'addition multi partie sécurisée [99] - La somme sécurisée [91].	Non	-Présenter un protocole pour k-means clustering, lorsque les données sont partitionnées horizontalement sur plusieurs parties. -Un nouveau protocole pour les données verticalement partitionnées pour plusieurs parties.
Privacy-Preserving Two-Party K-means Clustering via secure approximation [101]	2007	Horizontal	2	- Evaluation polynomiale aveuglée (oblivious polynomial evaluation) [98]. - Schéma homomorphe de Paillier [85] - Technique de l'approximation Sécurisée [102].	Non	-Amélioration de la sécurité, exactitude (correctness), normalisation des données et efficacité. -Protocole interactif avec normalisation des données.

Secure Two-Party k-means Clustering [103]	Novembre 2007	Arbitraire	2 (extensible)	<ul style="list-style-type: none"> - schéma homomorphe de Paillier [85] - Produit scalaire sécurisé [88] 	Non	<ul style="list-style-type: none"> -le plus sécurisé des protocoles dans le modèle semi honnête. -le protocole utilisé est compétitif en termes de coût de calcul et de communication, comparé aux protocoles précédents. -résoudre le pb de la division multi partie.
Large-scale k-means Clustering with User-Centric Privacy preservation. [104]	Mai 2008	Horizontal	n	<ul style="list-style-type: none"> - Cryptosystèmes homomorphes à clé publique de paillier [85] - Les parts aléatoires [46] - Le circuit d'évaluation de Yao [6] 	Oui	<ul style="list-style-type: none"> - L'introduction de l'idée de 'user-centric privacy preservation'. - Le calcul se fait dans chaque nœud et d'une façon asynchrone et insensible aux pannes. - Protocole scalable.
Distributed privacy preserving clustering with additive secret sharing [95]	2008	Vertical	$n > 3$	<ul style="list-style-type: none"> - Additive secret sharing [89] 	Oui	<ul style="list-style-type: none"> -Un nouveau protocole basé sur Additive secret sharing -L'utilisation du 'additive secret sharing' au lieu des cryptosystèmes homomorphes. -Des expériences sur des données réelles et synthétiques démontrant que le protocole proposé a un cout de calcul et de communication plus élevé.