*Лаба 1 Заготовка*

*ФИО*

Белов Матвей Алексеевич, Святковская Полина Борисовна (6113-100503D)

*Тема*

92;"Location Privacy; K-Anonymity; Anonymization "

Описание предметной области

Данный топик охватывает исследования в области конфиденциальности и анонимизации данных, в частности метод K-Anonymity, а также сведения о конфиденциальности местоположения. K-Anonymity — это метод конфиденциальности данных таким образом, что каждая запись в наборе данных неотличима от по крайней мере k-1 других записей. Концепция конфиденциальности местоположения может быть определена как право отдельных лиц решать, как, когда и для каких целей информация об их местоположении может быть передана другим сторонам.

*Недостаток*

В рассмотренных статьях нет информации о чётких стандартах доступа сервисов и сайтов к данным и в частности геоданным пользователя. Сайты могут собирать данные о пользователях через геотеги, что трудно обнаружить конечному пользователю, или же в коммерческих целях для подбора релевантной рекламы.

*Идея*

Предлагается создание единых стандартов безопасности данных, в которых разные «уровни доступа к информации» будут отражать к каким данным сайт/сервис будет иметь доступ для дальнейших хранения/обработки, сделав эту процедуру унифицированной и стандартизированной.

*Чистовик*

В современном мире мы часто сталкиваемся с приложениями, использующими наши данные, в том числе геоданные, такие как онлайн и оффлайн карты, банковские приложения и т.д. Известна концепция[1], [2] использования данных для работы подобных сервисов, однако появляется задача в защите персональных данных пользователя от незаконного распространяя его данных. Известны разные подходы[1]к этому вопросу(LPPMs)[3], в том числе к-анонимность [4], [5], имеющий точные значения затрачиваемых им ресурсов для обеспечения анонимности, вычислимые формулами для каждый задачи[6], и его подвид-к-анонимность на основе «credible chain»[7]. Эта модель крайне популярна, однако имеет ряд существенных недостатков[7], таких как лёгкая взламываемость по определённому алгоритму. На замену этому методу существует л-многообразие[8], более безопасная модель анонимизации данных, а также настраиваемая модель к-анонимности[9] с двумя дополнительными параметрами. В рамках множественных сравнений[10] подходов к вопросу анонимности были также отмечены подходы KNN[3], иерархическое расширение данных[10], метод случайной перестановки[9].

Несмотря на обилие методов по анонимизации данных с разной сложностью обеспечения и степенью защиты, отсутствуют строгие правовые стандарты, которые смогли бы закреплять за сервисами хранение и распространение лишь определённых типов данных пользователя. К примеру, сайт может собирать информацию о местоположении пользователя по геотегам медиафайлов.

Поэтому в настоящей статье мы предлагаем создать единые стандарты безопасности данных, в которых разные «уровни доступа к информации» будут отражать к каким данным сайт/сервис будет иметь доступ для дальнейших хранения/обработки. Этот подход заменит нынешние «Политики конфиденциальности» и «пользовательские соглашения на обработку персональных данных», сделав эту процедуру унифицированной и стандартизированной, пользователь будет сразу понимать, какие данные потребуются для работы с сервисом, и как именно будут храниться и распространяться его данные.

Список литературы:

[1] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, и J.-P. Hubaux, «Quantifying Location Privacy», в*2011 IEEE Symposium on Security and Privacy*, Oakland, CA, USA: IEEE, май 2011, сс. 247–262.doi: 10.1109/SP.2011.18.

[2] B. Liu, W. Zhou, T. Zhu, L. Gao, и Y. Xiang, «Location Privacy and Its Applications: A Systematic Study», *IEEE Access*, т. 6, сс. 17606–17624, 2018, doi: 10.1109/ACCESS.2018.2822260.

[3] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, и A. Iyengar, «Location Privacy-preserving Mechanisms in Location-based Services: A Comprehensive Survey», *ACM Comput. Surv.*,т. 54, сс. 1–36, янв. 2021, doi: 10.1145/3423165.

[4] L. Sweeney, «k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY», *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, т. 10, вып. 05, сс.557–570, окт. 2002, doi: 10.1142/S0218488502001648.

[5] B. Gedik и L. Liu, «Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms», *IEEE Trans. Mob. Comput.*,т. 7, вып. 1, сс.1–18, янв. 2008, doi: 10.1109/TMC.2007.1062.

[6] A. Meyerson и R. Williams, «On the complexity of optimal K-anonymity», в*Proceedings of the twenty-third ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, Paris France: ACM, июн. 2004, сс.223–228.doi: 10.1145/1055558.1055591.

[7] H. Wang, H. Huang, Y. Qin, Y. Wang, и M. Wu, «Efficient Location Privacy-Preserving k-Anonymity Method Based on the Credible Chain», *ISPRS Int. J. Geo-Inf.*, т. 6, вып. 6, с. 163, июн. 2017, doi: 10.3390/ijgi6060163.

[8] A. Machanavajjhala, J. Gehrke, D. Kifer, и M. Venkitasubramaniam, «L-diversity: privacy beyond k-anonymity», в*22nd International Conference on Data Engineering (ICDE’06)*, Atlanta, GA, USA: IEEE, 2006, сс. 24–24.doi: 10.1109/ICDE.2006.1.

[9] L. Liu, «A Customizable k-Anonymity Model for Protecting Location Privacy».

[10] A. Khoshgozaran, C. Shahabi, и H. Shirani-Mehr, «Location privacy: going beyond K-anonymity, cloaking and anonymizers», *Knowl. Inf. Syst.*, т. 26, вып. 3, сс. 435–465, мар. 2011, doi: 10.1007/s10115-010-0286-z.