Jurnal Bisantara Informatika (JBI)
Vol.8, No.2, Desember 2024, pp. 1~6
ISSN (print): 2686-6455, ISSN (online): 2686-5319

Kajian Literatur Sistematis : Perkembangan Metode Privasi Pempublikasian Data pada Data Media Sosial

M. Nur Khawarzimi*[1], Muhammad Fikri[2], Fahrur Riza Priyana[3], Rizkima Akbar Setiawan[4], Awansah[5], Nadia Julian Putri[6]
[1,2,3,4,5,6]Jurusan Teknik Elektro, Fakultas Teknik, Universitas Lampung, Lampung, Indonesia
e-mail: *[1]mnkhawarizmi@eng.unila.ac.id, [2]laniakea@eng.unila.ac.id, [3]fahrurrizap@eng.unila.ac.id [4]rizkimaakbarsetiawan@eng.unila.ac.id, [5]awansah@eng.unila.ac.id, [6]nadiajulian@eng.unila.ac.id

Abstrak

Peningkatan signifikan dalam penggunaan layanan media sosial telah menghasilkan sejumlah besar data yang dihasilkan pengguna. Data yang dihasilkan oleh pengguna dibagikan kepada publik untuk tujuan seperti menganalisis perilaku konsumen, melacak penyebaran penyakit, menganalisis pandangan politik, dan sebagainya. Data tersebut menarik perhatian banyak pihak, seperti perusahaan periklanan, pemerintah, penambang data, atau bahkan pihak yang mempunyai niat buruk. Disisi lain mekanisme publikasi ini menimbulkan ancaman terhadap privasi penggunanya. Banyak penelitian telah dilakukan berupaya memberikan solusi untuk melindungi privasi namun, tinjauan sistematis terhadap dinamika penelitian privasi di media sosial dan temuan pendekatan terbaru terhadap solusi privasi dari perspektif yang lebih luas masih belum dieksplorasi dalam literatur saat ini. Melalui metodologi tinjauan pustaka yang sistematis dengan analisis kualitatif, penelitian bertujuan untuk menemukan kesenjangan penelitian dan mengidentifikasi potensi pengembangan metode dan arah penelitian di masa depan mengenai solusi perlindungan privasi data di media sosial. Hasil penelitian berupa kajian state of the art pada perlindungan privasi dalam pempublikasian data, ancaman privasi, metriks untuk mengukur efektifitas metode perlindungan privasi dan masalah yang timbul dari perlindungan privasi seperti menurunya utilitas data dan informasi yang hilang

Kata kunci. *Graph Anonymization, Privacy Preserving Data Publication, Social graph.*

1. PENDAHULUAN

Dewasa ini, media sosial menjadi sangat populer karena fitur-fiturnya yang bermanfaat. Penggunanya dapat dengan bebas mengakses platform tersebut dan menggunakannya untuk berbagi pemikiran, mendapatkan informasi, dan terhubung dengan orang lain. Setiap hari jejaring sosial menghasilkan sejumlah besar data yang diposting oleh pengguna. Data yang diekstrak dari platform media sosial dapat dianalisis di berbagai bidang untuk menghasilkan informasi yang berguna, misalnya untuk memahami tren sosial, sentimen, dan perilaku masyarakat. Penyedia layanan media sosial sebagai pemilik kumpulan data pengguna memiliki hak atas publikasi dan berbagi data kepada pihak lain seperti pemerintah, analis data, peneliti, atau perusahaan iklan. Praktik saat ini dalam penerbitan atau pempublikasian data terutama bergantung pada kebijakan dan pedoman mengenai jenis data apa saja yang dapat dipublikasikan dan pada kesepakatan tentang penggunaan data yang dipublikasikan [1].Pengumpulan informasi digital oleh pemerintah, perusahaan, dan individu telah menciptakan peluang untuk pengambilan keputusan berbasis pengetahuan dan informasi. Didorong oleh manfaat bersama, atau oleh peraturan yang mengharuskan data tertentu untuk dipublikasikan, ada permintaan untuk pertukaran dan publikasi data di antara berbagai pihak. Namun demikian,

data dalam bentuk aslinya, biasanya mengandung informasi sensitif tentang individu, dan mempublikasikan data tersebut akan melanggar privasi individu.

Keamanan data merupakan aspek penting dalam melindungi dan menjamin keutuhan maupun kerahasiaan data yang berisi informasi penting. Dalam meningkatkan aspek keamanan dan menjaga kerahasiaan informasi dan kerahasiaan dari suatu data file dokumen dapat dilakukan sistem keamanan kriptografi, yaitu dengan menyandikan isi atau content file pada data tersebut menjadi isi yang sulit bahkan tidak dapat dipahami melalui dengan proses enkripsi dan untuk memperoleh kembali informasi yang asli dilakukan proses dekripsi [2].

Privasi merupakan hak individu untuk memiliki kendali atas bagaimana informasi pribadi digunakan. Secara umum data pribadi memuat dua informasi yaitu identitas dan atribut. Identitas merupakan informasi bersifat unik yang melekat pada individu seperti nama, umur, jenis kelamin. Sedangkan, atribut merupakan informasi pribadi terkait individu yang bersifat sensitif, seperti riwayat penyakit, hubungan keluarga, rencana kegiatan, riwayat pembelian produk atau jasa dan lokasi. Selanjutnya, masalah data privasi dapat diidentifikasi berdasarkan dua jenis pengungkapan informasi. Pertama, pengungkapan identitas (*identity disclosure*) yakni mengungkapkan identifikasi entitas dengan pengetahuan latar belakang tertentu yang diketahui oleh penyerang. Kedua, pengungkapan atribut (*attribute disclosure*) terjadi ketika penyerang dapat menyimpulkan beberapa informasi baru mengenai individu berdasarkan data yang dirilis. Pengungkapan informasi ini dapat dikategorikan sebagai serangan kebocoran privasi [3].

Data pribadi dalam media sosial berjenis data relasional yang dimodelkan dalam bentuk graf sosial, memungkinkan pengguna dapat terhubung dengan suatu relasi ke individu lainnya, yang direpresentasikan dengan simpul *(nodes)* yang terhubung dengan tepi (*edge*). Aktifitas pengguna di media sosial juga terekam dalam informasi pada data graf sosial, hal ini menjadikan data graf pada media sosial kaya akan informasi yang dapat ditambang dan dianalisa untuk berbagai kepentingan seperti studi sosial, studi perilaku konsumen, studi penyebaran penyakit dan lain sebagainya, namun data yang dipublikasikan dan dibagi kepada pihak lain, akan menimbulkan masalah privasi yang mengancam penggunanya. Disisi lain memberikan perlindungan privasi pada data akan mempengaruhi kualitas data yang dilindungi seperti informasi yang hilang atau kualitas data yang buruk. Maka dari itu, diperlukan upaya dalam mengembangkan metode dan perangkat untuk mempublikasikan data sehingga data yang dipublikasikan tetap bermanfaat secara teknis, sementara privasi individu tetap terjaga. Upaya ini disebut dengan *Privacy Preserving Data Publishing* (PPDP) [4]. Belakangan ini, perlindungan privasi dalam publikasi data atau PPDP mendapat perhatian yang cukup besar dari para peneliti. Para peneliti mengusulkan banyak solusi untuk mengamankan data privasi pengguna tinjauan sistematis tentang dinamika penelitian PPDP dan temuan-temuan terbaru dalam pendekatan perlindungan privasi dari perspektif yang lebih luas belum tereksplorasi dalam literatur terkini [5]. Oleh karena itu, penulis menyajikan analisis komprehensif dinamika perkembangan berbagai solusi yang telah diusulkan untuk mengatasi masalah privasi di media sosial.

Kajian literatur sistematis pada penelitian ini dilakukan dalam konteks penelitian dalam mengembangkan metode perlindungan privasi pada data graf di media sosial. Pengembangan metode diharapkan dapat memberi kontribusi terhadap penelitian di bidang perlindungan privasi pada data graf. Tujuan kajian literatur sistematis dalam penelitian ini diantara lain adalah sebagai berikut:

1. Menemukan model, teknik atau metode perlindungan privasi pada data graf di media sosial
2. Menemukan keterbatasan penelitian – penelitian terdahulu (*research gap*)
2. Melakukan sintesis hasil pengukuran metrik privasi dan utilitas data
3. Memperkirakan arah dan potensi pengembangan penelitian

Corresponding author * **M. Nur Khawarzimi**

2. METODE PENELITIAN

Dalam penelitian ini digunakan metode penelitian dengan pendekatan kajian literatur Sistematis atau *Systematic Literature Review* (SLR) yang dilakukan untuk mengumpulkan dan mengevaluasi penelitian yang berkaitan dengan topik tertentu. Metode ini merupakan cara sistematis untuk mengumpulkan, mengevaluasi secara kritis, mengintegrasikan, dan menyajikan temuan dari berbagai kajian penelitian mengenai pertanyaan penelitian atau suatu topik. SLR menilai tingkat kualitas bukti (evidence-based) yang tersedia pada suatu pertanyaan atau topik yang diminati. SLR dapat memberikan level pemahaman yang lebih luas dan akurat dibandingkan tinjauan literatur pada umumnya. Penulis menggunakan metode tinjauan sistematis literatur oleh Kitchenham [4] dan [5] yang membagi proses menjadi beberapa langkah diantara lain :

2.1 Research Quesiton

SLR pada penelitian ini dilakukan dalam konteks penelitian metode perlindungan privasi dalam pempublikasian data media sosial. Tujuan utama dalam melakukan SLR dalam penelitian ini adalah: menyintesis metode perlindungan privasi pada media sosial yang telah diusulkan oleh penelitian terdahulu, menyintesis metrik pengukuran kualitas perlindungan privasi dalam pempublikasian data media sosial, menemukan metode yang paling efektif dalam perlindungan privasi, serta menemukan keterbatasan penelitian penelitian terdahulu. Pertanyaan penelitian dibuat berdasarkan kebutuhan dari topik yang dipilih untuk menjaga fokus proses kajian sietematis, Pertanyaan penelitian pada penelitian ini dirumuskan dengan menggunakan pendekatan PICOC (*Population, intervention, comparison, outcome and context*). Pertanyaan penelitian dirumuskan sebagai berikut :

RQ 1: Model ancaman atau serangan seperti apa yang mengancam privasi pada data graf di media sosial?
RQ 2: Solusi perlindungan privasi seperti apa yang telah diusulkan pada penelitian terdahulu ?
RQ 3: Jenis data apa saja di media sosial yang rentan terhadap ancaman privasi?
RQ 4: Bagaimana dinamika pengembangan metode perlindungan privasi dalam pemublikasian data media sosial ?

2.2 Pencarian Referensi

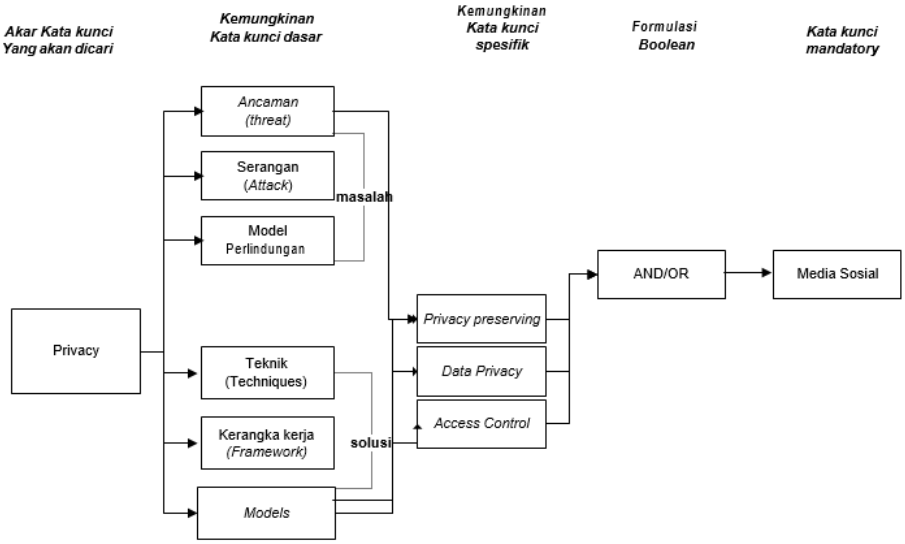
Melalui kajian sistematis secara komprehensif penulis melakukan kajian literature untuk menghasilkan sumber sumber yang relevan untuk menjawab pertanyaan penelitian, dan referensi terkait lainnya melalui database penelitian secara elektronik. Penulis telah melakukan seleksi dan menetapkan lima database publikasi ilmiah elektronik yang memiliki kredibilitas dan kualitas publikasi penelitian terbaik diantarannya ditunjukan pada Tabel I.

Tabel I. Database Penelitian Elektronik

No	Database	Tautan
1.	ScienceDirect	http://www.sciencedirect.com/science/search
2.	IEEE Xplore	http://ieeexplore.ieee.org/search/advsearch.jsp
3.	ACM Digital Library	http://dl.acm.org/advsearch.cfm?
4.	SpringerLink	http://link.springer.com/advanced-search
5.	Scoupus	http://www.scoupus.com/

Proses pencarian literatur dilakukan melalui proses *snowballing* yaitu pencarian literatur yang mengacu pada literatur awal (*forward snowballing*), maupun mencari literatur yang menjadi referensi dari literature awal (*backward snowballing*). Selain itu rekomendasi peneliti

ahli (peneliti yang telah berkontribusipada topik penelitian yang dipilih terbanyak dengan jumlah citasi jurnal yang tinggi) juga dapat dijadikan pelengkap sumber literatur. Untuk menemukan literatur yang sesuai dengan topik yang diambil, strategi penelusuran yang dilakukan adalah dengan menetukan *search string* (Frasa pencarian) pada kueri metadata dari database penelitian. Kemudian menyusun terminologi yang digunakan dalam menentukan kata kunci pencarian ditunjukan pada gambar 1



Gambar 1 Pencarian kata kunci berdasarkan susunan terminologi

2.3 Kriteria pemilihan dan penyaringan Literatur

Setelah dilakukan proses pencarian literatur selanjutnya kumpulan literatur dikompilasi dan dilakukan proses seleksi. Proses seleksi dilakukan dalam beberapa tahap, meliputi identifikasi (*identification*), penyaringan (*screening*), penilaian kelayakan (*eligibity*) dan penyertaan ke dalam sintesis (*include*). Untuk mengurangi bias, maka dikembangkan kriteria kriteria untuk memasukan (*inclusion*) atau mengeluarkan (*exclusion*) suatu literature dari daftar yang telah disusun ditunjukan melalui tabel 2.

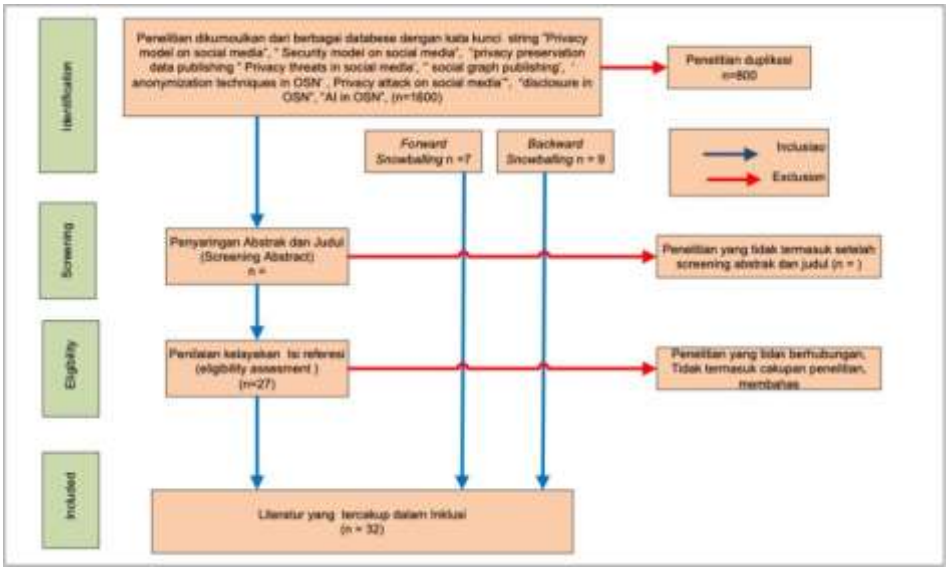
Tabel 2. Kriteria pemilihan dan penyaringan literatur

Tahap	**Konten yang diperiksa**	**Kriteria**	**Keterangan**
Identification	Judul dan tahun terbit	Inclusion	I.1. Literatur yang diperoleh dari hasil pencarian dengan search string *I.2* Literatur tambahan yang diperoleh dari hasil proses *snowballing* I.3 Literatur dipublikasikan antara tahun 2014- 2024

	Terpublikasi antara tahun 2014 hingga 2024	Exclusion	E.1 Literatur yang duplikat dengan memeriksa judul, penulis, tahun terbit dan nama konferensi Literatur bukan merupakan jurnal/ conference paper/ bukuteks
Screening	Judul, abstrak, keywords, nama konfrensi ataujurnal	Inclusion	*I.4.* Keywords atau abstrak mengandung salah satu frasa: *Privacy preserving, Privacy attack, Inference attack, Privacythreat in social media, anonymization techniques in Social media, privacy attack on social media, social graph publishing, disclosure in social media, AI in OSN* *I.5. Jurnal/paper conference terindeksscopus*
		Exclusion	E.3. Literatur merupakan studi sekunder (SLR, Systematic review atau meta analisis) E.4. Literatur tidak menggunakan bahasa inggris E.5. Literatur tidak memenuhi kriteria I.4 dan I.5
Eligibility	Isi Literatur	Inclusion	I.6. Literatur mampu menjawab minimal satu pertanyaan penelitian I.7. Literatur membahas tentang model keamanan
	Isi Literatur	Exclusion	E.6. Literatur tidak mampu menjawab satupun pertanyaan penelitian E.7 Penelitian tidak membahas serangan privasi pada data graf sosial
Included		Inclusion	I.7. Literaatur yang telah lolos seleksi pada tahap eligibility
		Exclusion	-

2.4 pemilihan dan penyaringan Literatur

Hasil pencarian dari lima database publikasi ilmiah diperoleh 300 literatur yang berpotensi relevan dengan penelitian. Hasil pencarian dan pemilihan katalog literatur memuat informasi kode identitas literatur, judul literatur, nama penulis, nama konferensi atau jurnal "tahun publikasi", kata kunci dan abstrak. Untuk menambah informasi yang diperlukan, proses snowballing ditambahkan dalam katalog literatur. Pada tahap akhir didapatkan sebanya 64 literatur yang akan digunakan untuk analisis kualitatif. Hasil pencarian dan pemilihan literatur disajikan pada gambar 2.



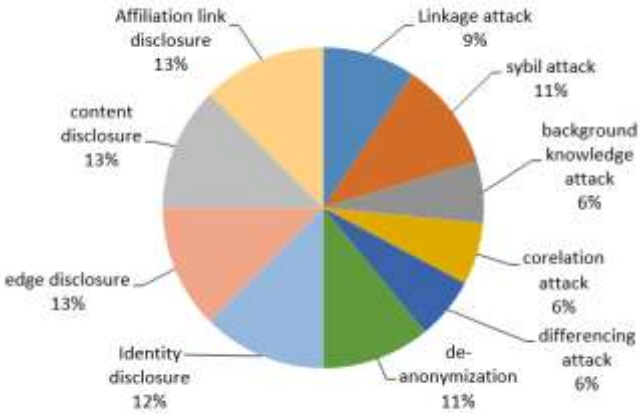
Gambar 2 Hasil Pencarian dan pemilihan literatur

3. HASIL DAN PEMBAHASAN

analisis dari hasil sintesis data bertujuan untuk menjawab pertanyaan penelitian yang telah ditetapkan sebelumnya yang terdiri dari RQ1 sampai dengan RQ4.

RQ 1: Jenis data pribadi apa saja di media sosial yang rentan terhadap ancaman pribadi ?
Melalui penghitungan tabulasi dari hasil kajian sistematis, dididentifikasi terdapat empat jenis data media sosial yang dibahas dan dijadikan objek penelitian dalam melakukan perlindungan privasi yaitu: data identitas, data spatiotemporal, data konten, dan data sosial. Frekuensi jenis data sosial paling banyak dilakukan penelitian yaitu sekitar 45 persen. Sementara itu data identitas sebesar 40,27 persen, data konten sebanyak 12 persen, dan data spatiotemporal sebanyak 23,16 persen

RQ 2: Model ancaman atau serangan apa yang mengancam privasi pada data graf media sosial?

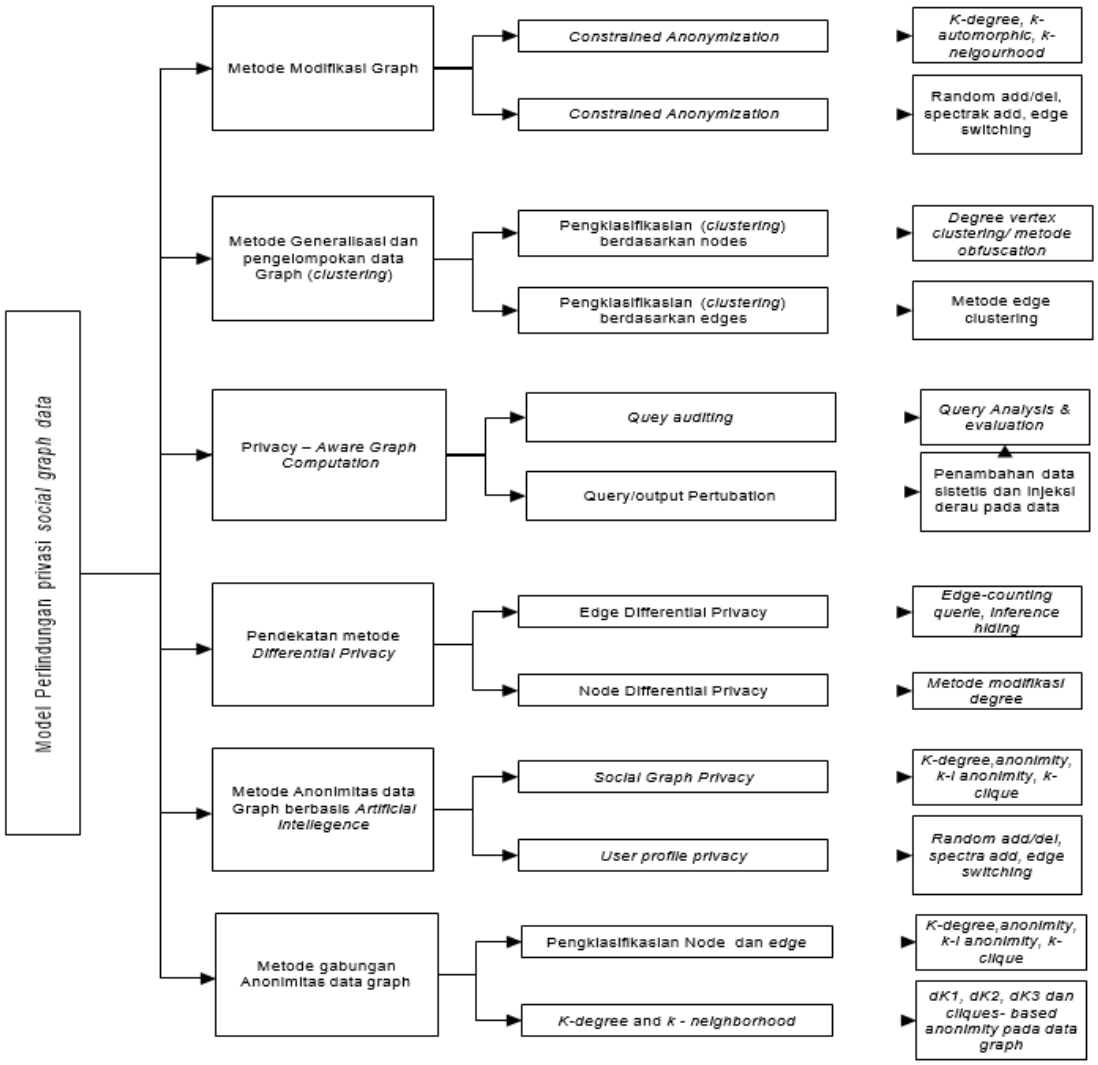


Gambar 3. Grafik tabulasi kajian sistematis serangan privasi pada data graf media sosial

Melalui penghitungan tabulasi dari hasil kajian sistematis, di identifikasi terdapat sepuluh jenis serangan privasi pada data graf di media sosial yang dibahas dalam penelitian: *Identity*

disclosure, edge disclosure, content disclosure,affiliation link disclosure, linkage attack, sybil attack, background knowledge attack, correlation attack, differencing attack, dan de-anonymization attack.

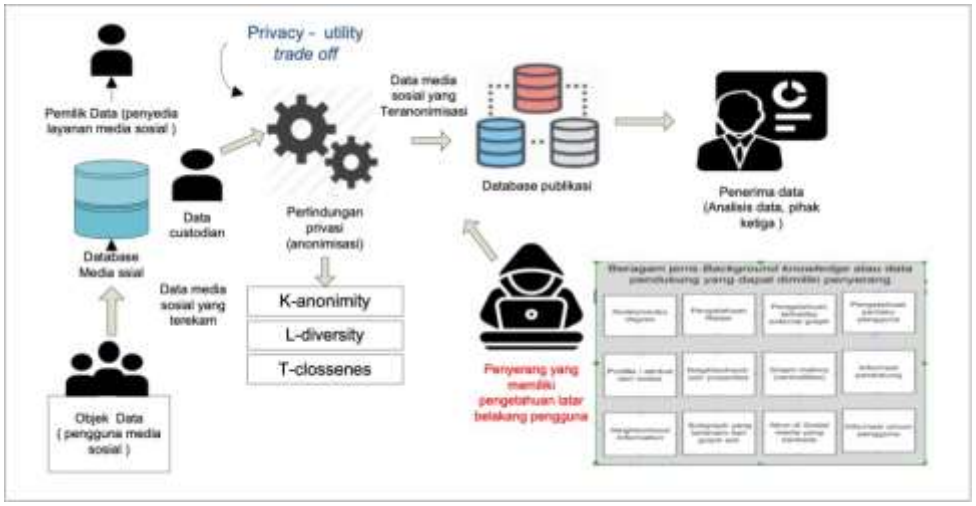
RQ 3: Solusi perlindungan privasi pada pempublikasian data media sosial apa yang telah diusulkan ?



Gambar 4. Taksonomi perlindungan privasi data graf

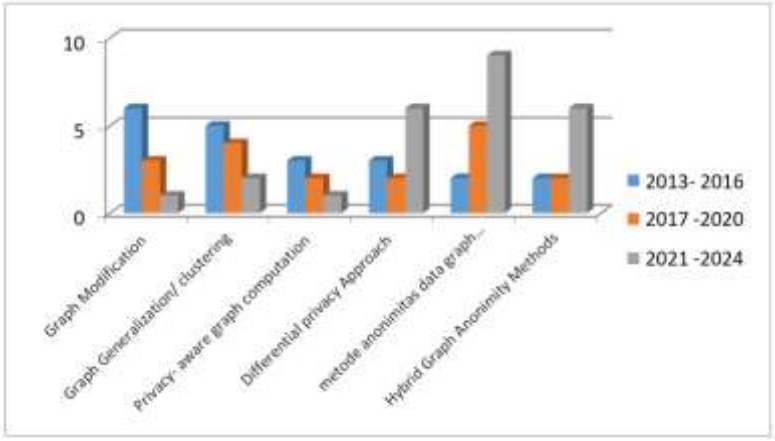
Berdasarkan hasil penelusuran literatur mengenai solusi perlindungan privasi pada data sosial graf di media sosial, peneliti mengelompokkan model perlindungan privasi data graf seperti yang diilustrasikan pada gambar 4. Adapun pengelompokkan metode perlindungan privasi data graf adalah sebagai berikut: modifikasi graf, generalisasi dan pengelompokkan graf, privacy-aware graph computation, differential privacy, anonimisasi data graf berbasis AI, dan penggabungan anonimitas data graf.

RQ 4 : Bagaimana dinamika pengembangan metode perlindungan privasi dalam pemublikasian data media sosial ?



Gambar 5. Mekanisme serangan dan perlindungan privasi pada pempulikasian data media sosial secara umum

Perlindungan privasi dalam pempulikasian data (PPDP) merupakaan kajian yang membahas seperangkat alat, metode, solusi, dan kerangka kerja untuk berbagi informasi berharga dengan analis dan peneliti tanpa membahayakan privasi pengguna [7]. Perancangan perlindungan privasi pada publikasi data media sosial memiliki proses seperti terlihat pada Gambar 5. Berdasarkan gambar 5 dataset media sosial dikumpulkan dari aktivitas pengguna dan dicatat dalam database yang dimiliki oleh penyedia layanan media sosial. Dataset yang akan dipublikasikan dikelola oleh data kustodian, yaitu pihak yang bertanggung jawab mengelola pendistribusian data. Publikasi data diatur sesuai kebijakan antara berbagai pihak, dalam hal ini pengguna jasa dan penyedia layanan media sosial. Proses perlindungan privasi dilakukan sebelum data dipublikasikan atau dibagikan kepada penerima. Perlindungan privasi yang dilakukan merupakan proses anonimisasi dengan berbagai metode dan algoritma yang mempertimbangkan keseimbangan antara efektivitas metode perlindungan privasi dan kegunaan data yang akan dipublikasikan. Data pengguna media sosial yang dianonimkan dipublikasikan kepada penerima seperti analis data, peneliti, lembaga pemerintah, dan sebagainya. Serangan privasi masih dapat terjadi pada data yang dianonimkan jika penyerang memiliki informasi latar belakang pengguna



Gambar 6. Grafik jumlah referensi metode berdasarkan tahun publikasi

Penulis merangkum hasil telusur literatur kedalam tabel, grafik, dan teks. Penulis mengelompokan hasil temuan berupa 64 referensi kemudian mensitesisnya sehingga didapatkan 4 referensi utama berdasarkan metode perlindungan privasi pada data graf yang dikaji kemudian

mengurutkannya berdasarkan tahun publikasi yang ditunjukan pada pengelompokan tahun publikasi dibagi kedalam tiga tahun dengan maksud untuk mengetahui fluktuasi publikasi selama tiga tahun ditunjukan pada gambar 6, dari hasil penghitungan diketahui bahwa terjadi peningkatan dan penurunan publikasi yang cukup signifikan pada masing masing metode perlindungan privasi. Rangkuman referensi masing masing metode ditunjukan pada tabel 3.

Tabel 3**.** Ringkasan referensi

Reference	Metode	Keunggulan	Jenis kajian	Teknik
J. H. Abawajy et. al [7]	Artificial Intelligence	Memprediksi tingkat detail untuk setiap keputusan berbagi di media sosial	konseptual	Logistic Regression
S.Rajabzadeh et.al[8]	Differential Privacy (DP)	Memecahkan masalah Atribut Sensitif yang berlipat ganda dalam Pempublikasian data	Teknikal	NB, SVM, RF
M. Siddula [9]	Graph Clustering	Perlindungan privasi yang superior dalam pempublikasian data	Teknikal	K-means algorithm
K. Li et. al [10]	Graph Modification	Utilitas data dan perlindungan privasi mencapai titik *trade-off*	Teknikal	K-match algorithm

4. KESIMPULAN

Perlindungan privasi dalam pempublikasian data media sosial merupakan area penelitian yang dinamis dengan banyak tantangan yang masih harus dipecahkan. Berbagai modifikasi metode anonimisasi telah dikembangkan oleh banyak peneliti. Namun,masih kurang dalam melindungi privasi dalam penerbitan data. Selain itu juga mekanisme privasi untuk serangan pengungkapan konten dan atribut masih menjadi kendala utama sehingga menjadi pertimbangan yang penting dalam mengembangkan metode terbaru. Metode anonimitas data graf berbasis AI dan metode anonimitas hybrid memiliki kecendrungan publikasi yang meningkat, metode modifikasi graf, metode pengelompokan dan metode komputasi memiliki kecendrungan jumlah publikasi yang menurun, sehingga dapat disimpulkan arah penelitian dan potensi pengembangan penelitian.

DAFTAR PUSTAKA

[1] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, “Privacy-preserving data publishing: A survey of recent developments,” *ACM Comput. Surv.*, vol. 42, no. 4, pp. 1–53, Jun. 2010, doi: 10.1145/1749603.1749605.

[2] Manullang, S. and Sembiring, J., 2023. Pengamanan Data File Dokumen Menggunakan Algoritma Advanced Encryption Standard Mode Chiper Block Chaining. *Antivirus: Jurnal Ilmiah Teknik Informatika, 17*(1), pp.53-67.

[3] M. Qi and D. Edgar-Nevill, "Social networking searching and privacy issues," *Information Security Technical Report*, vol. 16, no. 2, pp. 74–78, May 2011, doi: 10.1016/j.istr.2011.09.005.

[4] Yidong Li and Hong Shen, "On Identity Disclosure Control for Hypergraph- Based Data Publishing," *IEEE Trans.Inform.Forensic Secur.*, vol. 8, no. 8, pp. 1384–1396, Aug. 2013, doi: 10.1109/TIFS.2013.2271425.

[5] B. Kitchenham, "Procedures for Performing Systematic Reviews," p. 34.

[6] Computer Science and Information Technology, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, India, P.P. Churi, A. V. Pawar, and Computer Science and Information Technology, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, India, "A Systematic Review on Privacy Preserving DataPublishing Techniques," *JESTR*, vol. 12, no. 6, pp. 17–25, Dec. 2019, doi:10.25103/jestr.126.03.

[7] P. V. Torres-Carrion, C. S. Gonzalez-Gonzalez, S. Aciar, and G. Rodriguez- Morales, "Methodology for systematic literature review applied to engineering and education," in *2018 IEEE Global Engineering Education Conference (EDUCON)*, Tenerife, Apr. 2018, pp. 1364–1373. doi: 10.1109/EDUCON.2018.8363388.

[8] J. H. Abawajy, M. I. H. Ninggal, and T. Herawan, "Privacy Preserving SocialNetwork Data Publication," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 1974–1997, 2016, doi: 10.1109/COMST.2016.2533668.

[9] S. Rajabzadeh, P. Shahsafi, and M. Khoramnejadi, "A graph modification approach for k-anonymity in social networks using the genetic algorithm,"*Soc. Netw. Anal. Min.*, vol. 10, no. 1, p. 38, Dec. 2020, doi: 10.1007/s13278-020-00655-6.

[10] M. Siddula, Y. Li, X. Cheng, Z. Tian, and Z. Cai, "Anonymization in Online Social Networks Based on Enhanced Equi-Cardinal Clustering," *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 4, pp. 809–820, Aug. 2019, doi: 10.1109/TCSS.2019.2928324.

[11] K. Li, G. Luo, Y. Ye, W. Li, S. Ji, and Z. Cai, "Adversarial Privacy- Preserving Graph Embedding Against Inference Attack," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6904–6915, Apr. 2021, doi: 10.1109/JIOT.2020.3036583.

Corresponding author * **M. Nur Khawarzimi**