ELANG: Journal of Interdisciplinary Research
E-ISSN: 3025-2482

Evolusi Autentikasi Mobile dari Password ke Artificial Intelligence dan Kriptografi Modern: Analisis Bibliometrik Publikasi Scopus 1997–2026

Kholilur Rohman[1], Dimas Bagas Firmansyah Arifin[2], Tamara Adjuah[3], Hozairi[4]
[1)]kholilurrohma23ti@uim.ac.id || [2)]dimasbagas23ti@uim.ac.id || [3)]tamaraadjuah@gmail.com || [4)]dr.hozairi@gmail.com

[1,2,3,4]*Universitas Islam Madura, Fakultas Teknik, Program Studi Teknik Informatika, Pamekasan Madura, Indonesia*

Kata Kunci

Authentication Methods; Bibliometric Analysis; Cryptography; Mathematical Biometric Authentication; Mobile Security; VOSviewer.

Author Korespondensi
kholilurrohma23ti@uim.ac.id

Abstrak

Penelitian ini bertujuan memetakan perkembangan penelitian mengenai metode *authentication* berbasis matematika pada keamanan aplikasi *mobile* menggunakan pendekatan bibliometrik. Metode autentikasi berbasis matematika dalam penelitian ini mencakup kriptografi, fungsi hash, model probabilistik, autentikasi biometrik berbasis statistik, serta integrasi *machine learning*. Data diperoleh dari basis data *Scopus* menggunakan kata kunci terkait autentikasi, keamanan mobile, biometrik, dan kriptografi. Setelah proses *screening* dan *cleaning*, diperoleh 840 publikasi periode 1997–2026 yang dianalisis menggunakan VOSviewer melalui *co-occurrence analysis*, *co-authorship analysis*, *citation analysis*, serta *visualisasi network*, *overlay*, dan *density*. Analisis kata kunci menggunakan *minimum occurrence threshold* sebesar 5 kemunculan. Hasil penelitian menunjukkan bahwa jumlah publikasi meningkat secara signifikan sejak tahun 2014 dan mencapai puncaknya pada tahun 2025. Analisis overlay visualization mengidentifikasi evolusi topik dari autentikasi berbasis kata sandi menuju autentikasi biometrik, kecerdasan buatan, dan protokol kriptografi *modern*. *Network* visualization menunjukkan keterkaitan yang kuat antara *authentication*, *biometric authentication*, *artificial intelligence*, dan *public key cryptography*, sedangkan *density visualization* mengungkap bahwa autentikasi biometrik masih menjadi fokus utama dengan topik baru seperti *liveness detection* dan *anti-spoofing* yang menunjukkan tren pertumbuhan tinggi. Penelitian ini memberikan kontribusi dengan memetakan hubungan antara pendekatan matematis dan perkembangan teknologi autentikasi *mobile*. Namun, penelitian ini terbatas pada penggunaan basis data Scopus sehingga belum mencakup seluruh publikasi yang tersedia pada basis data lain.

1. Pendahuluan

Perkembangan pesat teknologi komunikasi dan komputasi telah mendorong peningkatan signifikan dalam penggunaan aplikasi *mobile* pada berbagai sektor, seperti perbankan digital, kesehatan, pendidikan, perdagangan elektronik, dan layanan publik. Transformasi digital tersebut menjadikan keamanan informasi sebagai aspek yang sangat penting, terutama dalam proses verifikasi identitas pengguna sebelum memperoleh akses ke sistem. Autentikasi merupakan mekanisme utama yang digunakan untuk memastikan bahwa pengguna yang mengakses sistem adalah pihak yang berwenang. Meskipun metode autentikasi konvensional berbasis kata sandi (*password*) dan *Personal Identification Number* (PIN) masih banyak digunakan, berbagai laporan keamanan menunjukkan bahwa kredensial yang dicuri, digunakan ulang, atau diperoleh melalui serangan *phishing* masih menjadi salah satu penyebab utama pelanggaran keamanan data dan pengambilalihan akun pengguna (Hasan et al., 2025) . Kondisi tersebut mendorong pengembangan metode autentikasi yang lebih aman, adaptif, dan tahan terhadap berbagai bentuk serangan siber modern.

Dalam penelitian ini, *authentication* berbasis matematika didefinisikan sebagai mekanisme verifikasi identitas yang memanfaatkan prinsip-prinsip matematis, seperti kriptografi, fungsi hash, teori probabilitas, model statistik, optimisasi, serta algoritma *machine learning* untuk menjamin keaslian identitas pengguna dan keamanan pertukaran data. Pendekatan matematis ini menjadi fondasi berbagai metode *autentikasi modern*, mulai dari autentikasi kriptografis berbasis kunci publik, autentikasi biometrik berbasis pengenalan pola, hingga *continuous authentication* yang memanfaatkan analisis perilaku pengguna. Keunggulan utama pendekatan tersebut terletak pada kemampuannya dalam menyediakan jaminan keamanan formal, menjaga integritas data, serta meningkatkan efisiensi proses autentikasi pada lingkungan komputasi yang dinamis (Korać et al., 2025).

Kebutuhan akan sistem autentikasi yang tidak hanya aman secara kriptografis tetapi juga efisien dan adaptif terhadap keterbatasan perangkat mobile terus meningkat. Lingkungan mobile memiliki karakteristik khusus, seperti keterbatasan sumber daya komputasi, mobilitas tinggi, konektivitas yang dinamis, serta risiko kehilangan atau pencurian perangkat. Selain itu, data autentikasi sering kali mengandung informasi sensitif yang berkaitan dengan identitas pengguna sehingga aspek keamanan dan privasi menjadi perhatian utama dalam pengembangan aplikasi *modern* (Korać et al., 2025) . Oleh karena itu, diperlukan metode autentikasi yang mampu memberikan tingkat keamanan tinggi tanpa mengorbankan kenyamanan pengguna (*usability*) maupun kinerja sistem.

Berbagai penelitian telah mengembangkan pendekatan autentikasi *modern* untuk menjawab tantangan tersebut. (Hasan et al., 2025) mengelompokkan metode autentikasi ke dalam beberapa kategori utama, yaitu *password-based authentication*, *biometric authentication*, *behavioral authentication*, dan *multi-factor authentication*. Pada kelompok autentikasi biometrik, teknologi seperti *fingerprint recognition*, *face recognition*, dan *iris recognition* banyak digunakan karena mampu meningkatkan kenyamanan pengguna sekaligus memperkuat keamanan sistem. Namun demikian, pendekatan ini masih menghadapi tantangan berupa *spoofing attack*, *presentation attack*, dan isu privasi data biometrik (Yeovandi et al., 2025). Di sisi lain, *continuous authentication* berbasis perilaku pengguna mulai berkembang dengan memanfaatkan *machine learning* untuk melakukan verifikasi identitas secara berkelanjutan berdasarkan pola interaksi pengguna terhadap perangkat (Gilbert & Gilbert, 2025) . Selain itu, berbagai teknik matematis seperti fungsi hash, enkripsi simetris dan asimetris, *public key cryptography*, *probabilistic model*, serta *neural network* telah banyak diterapkan untuk meningkatkan ketahanan sistem autentikasi terhadap ancaman keamanan yang semakin kompleks (Hasija et al., 2025).

Meskipun penelitian mengenai autentikasi dan keamanan *mobile* berkembang sangat pesat, kajian yang memetakan perkembangan bidang tersebut secara menyeluruh masih relatif terbatas. Beberapa penelitian bibliometrik sebelumnya lebih banyak berfokus pada topik keamanan informasi secara umum. (Humaidi et al., 2025) melakukan analisis bibliometrik mengenai *Information Security Risk Management*, sedangkan (Hasija et

al., 2025) memetakan perkembangan penelitian pada bidang *Post-Quantum Cryptography*. Selain itu, (Kachbou et al., 2025) memanfaatkan pendekatan bibliometrik untuk menganalisis tren penelitian pada domain yang berbeda menggunakan *Scopus* dan VOSviewer. Meskipun memberikan gambaran yang bermanfaat mengenai perkembangan bidang masing-masing, penelitian-penelitian tersebut belum secara spesifik mengkaji keterkaitan antara kriptografi, autentikasi biometrik, *machine learning*, dan keamanan aplikasi *mobile* dalam satu kerangka analisis yang terintegrasi.

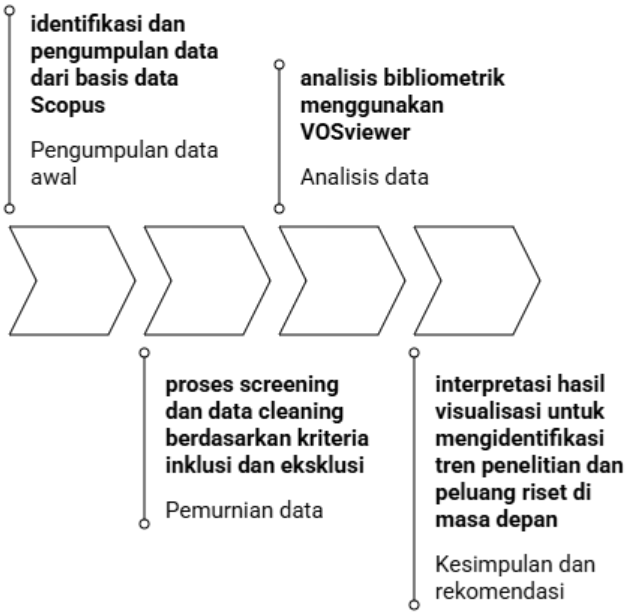
Perbedaan mendasar penelitian ini dibandingkan studi bibliometrik sebelumnya terletak pada fokus kajian yang secara khusus menempatkan metode autentikasi berbasis matematika sebagai objek utama analisis. Jika (Hasija et al., 2025) hanya berfokus pada perkembangan penelitian *post-quantum cryptography*, maka penelitian ini mencakup spektrum yang lebih luas, meliputi kriptografi, autentikasi biometrik berbasis model statistik, *behavioral authentication*, serta integrasi *machine learning* dalam sistem *autentikasi mobile*. Dengan demikian, penelitian ini tidak hanya memetakan perkembangan salah satu cabang teknologi keamanan, tetapi juga menganalisis hubungan antarpendekatan matematis yang membentuk ekosistem autentikasi *modern*.

Pendekatan bibliometrik dipilih karena tujuan penelitian ini bukan untuk mengevaluasi efektivitas suatu metode autentikasi tertentu sebagaimana dilakukan dalam *Systematic Literature Review* (SLR), melainkan untuk memetakan struktur intelektual, tren perkembangan penelitian, hubungan antar topik, kontribusi negara, serta arah evolusi bidang penelitian dalam skala yang luas. Menurut (Donthu et al., 2021) , analisis bibliometrik merupakan metode yang efektif untuk mengidentifikasi perkembangan ilmu pengetahuan secara kuantitatif dan objektif melalui analisis publikasi, sitasi, dan hubungan antar dokumen ilmiah. Oleh karena itu, pendekatan ini dinilai paling sesuai untuk menggambarkan lanskap penelitian autentikasi berbasis matematika pada keamanan aplikasi mobile secara komprehensif.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk melakukan analisis dan visualisasi bibliometrik terhadap publikasi ilmiah yang berkaitan dengan metode autentikasi berbasis matematika pada keamanan aplikasi mobile menggunakan database Scopus dan perangkat lunak VOSviewer. Hasil penelitian diharapkan dapat memberikan gambaran mengenai tren perkembangan penelitian, struktur intelektual bidang kajian, topik-topik dominan, serta peluang penelitian yang masih terbuka sehingga dapat menjadi referensi bagi peneliti dan pengembang sistem keamanan di masa mendatang.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode analisis bibliometrik untuk mengkaji perkembangan penelitian terkait metode authentication berbasis matematika pada keamanan aplikasi mobile. Analisis bibliometrik merupakan pendekatan yang digunakan untuk mengevaluasi struktur intelektual suatu bidang penelitian melalui analisis publikasi ilmiah secara sistematis, termasuk pola sitasi, kolaborasi penulis, hubungan antar topik penelitian, serta perkembangan tren penelitian dari waktu ke waktu (Donthu et al., 2021) . Pendekatan ini dipilih karena mampu memberikan gambaran yang komprehensif, objektif, dan terukur mengenai evolusi penelitian dalam suatu domain serta banyak digunakan untuk memetakan bidang ilmu yang berkembang pesat.



Gambar 1. Alur Penelitian

Alur penelitian terdiri atas empat tahap utama, yaitu: (1) identifikasi dan pengumpulan data dari basis data Scopus, (2) proses screening dan data cleaning berdasarkan kriteria inklusi dan eksklusi, (3) analisis bibliometrik menggunakan VOSviewer, dan (4) interpretasi hasil visualisasi untuk mengidentifikasi tren penelitian dan peluang riset di masa depan.

1. Sumber dan Pengumpulan Data
   Data penelitian diperoleh dari basis data Scopus sebagai sumber utama literatur ilmiah. Scopus dipilih karena memiliki cakupan multidisiplin yang luas, metadata yang lengkap, serta kompatibilitas yang tinggi dengan perangkat lunak analisis bibliometrik seperti VOSviewer dan Bibliometrix (Donthu et al., 2021) . Selain itu, Scopus menyediakan data sitasi yang relatif konsisten sehingga banyak digunakan dalam penelitian bibliometrik skala besar.
   Meskipun basis data lain seperti Web of Science dan IEEE Xplore juga banyak digunakan dalam penelitian keamanan siber dan kriptografi, penelitian ini hanya menggunakan Scopus untuk menjaga konsistensi metadata, mengurangi potensi duplikasi dokumen lintas indeks, serta mempermudah proses standarisasi data bibliografis. IEEE Xplore memiliki cakupan yang sangat kuat pada prosiding konferensi dan publikasi teknik, sedangkan Web of Science memiliki kebijakan indeksasi yang berbeda dengan Scopus. Oleh karena itu, penggunaan satu basis data dilakukan untuk menjaga homogenitas data yang dianalisis. Namun demikian, penggunaan Scopus sebagai sumber tunggal merupakan salah satu keterbatasan penelitian yang perlu diperhatikan dalam interpretasi hasil.
   Proses pencarian dilakukan pada Januari 2026 menggunakan *search string* yang dirancang untuk mencakup berbagai pendekatan autentikasi berbasis matematika pada lingkungan mobile sebagai berikut: TITLE-ABS-KEY (("*mobile* application" OR "*mobile* app" OR *smartphone* OR "*mobile* devices") AND (authentication OR "*user authentication*") AND ("*cryptographic authentication*" OR "*biometric authentication*" OR *cryptography* OR "*public key cryptography*")). Perluasan *search* string dilakukan untuk mengurangi risiko terlewatnya publikasi yang membahas metode matematis lain seperti *hash-based authentication*, *zero-knowledge proof*, *probabilistic model*, dan *machine learning* yang saat ini banyak digunakan dalam pengembangan sistem *autentikasi modern*.

Proses pencarian menghasilkan 840 dokumen yang memenuhi kriteria pencarian. Selanjutnya dilakukan proses *screening* berdasarkan jenis dokumen, bahasa, relevansi topik, serta kelengkapan metadata. Tahap *data cleaning* meliputi pemeriksaan duplikasi, penghapusan metadata yang tidak lengkap, dan standarisasi kata kunci agar diperoleh data yang konsisten untuk analisis bibliometrik. Seluruh dokumen yang memenuhi kriteria inklusi kemudian diekspor dalam format CSV dan dianalisis menggunakan VOSviewer.
Kriteria inklusi penelitian meliputi:

1. Artikel jurnal dan conference proceedings;
2. Ditulis dalam bahasa Inggris;
3. Terindeks dalam Scopus;
4. Rentang tahun publikasi 1997–2026;
5. Membahas autentikasi, keamanan mobile, atau metode matematis yang mendukung autentikasi.

2. Pengolahan dan Analisis Data
Sebelum dilakukan analisis, data terlebih dahulu melalui proses *data cleaning* untuk meningkatkan kualitas dan akurasi hasil. Tahapan ini meliputi penghapusan dokumen duplikat, pemeriksaan metadata yang tidak lengkap, serta standarisasi istilah kata kunci. Sebagai contoh, istilah "*biometric authentication*", "*biometrics*", dan "*biometric security*" diseragamkan ke dalam kelompok istilah yang sama untuk mengurangi redundansi visualisasi.
Proses *screening* dan validasi dokumen dilakukan oleh dua peneliti secara independen berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan. Ketidaksesuaian hasil seleksi diselesaikan melalui diskusi hingga diperoleh kesepakatan akhir. Pendekatan ini dilakukan untuk meningkatkan reliabilitas proses seleksi dokumen dan meminimalkan subjektivitas peneliti.
Analisis data dilakukan menggunakan perangkat lunak VOSviewer versi terbaru yang berbasis *Visualization of Similarities* (VOS) (Van Eck & Waltman, 2010) . Perangkat lunak ini digunakan untuk memetakan hubungan antar elemen bibliografis seperti penulis, dokumen, sitasi, maupun kata kunci. Pada analisis *overlay visualization*, nilai *Average Publication Year* (APY) dihitung secara otomatis oleh VOSviewer berdasarkan rata-rata tahun publikasi seluruh dokumen yang mengandung kata kunci tertentu. Nilai APY digunakan untuk mengidentifikasi tingkat kebaruan suatu topik penelitian, di mana nilai yang lebih tinggi menunjukkan kecenderungan topik yang lebih baru dalam literatur ilmiah.
Analisis bibliometrik yang dilakukan meliputi:

1. Co-authorship analysis untuk mengidentifikasi pola kolaborasi antar penulis dan institusi;
2. Co-occurrence analysis untuk menganalisis hubungan antar kata kunci;
3. Citation analysis dan co-citation analysis untuk mengidentifikasi publikasi yang berpengaruh;
4. Bibliographic coupling untuk mengidentifikasi keterkaitan dokumen berdasarkan referensi yang digunakan.

Dalam penelitian ini, *co-occurrence analysis* dipilih sebagai teknik utama karena tujuan penelitian adalah memetakan hubungan konseptual antar topik dan mengidentifikasi perkembangan tema penelitian autentikasi berbasis matematika. Berbeda dengan citation analysis yang berfokus pada pengaruh publikasi tertentu, co-occurrence analysis lebih sesuai untuk mengungkap struktur pengetahuan dan evolusi topik penelitian dalam suatu bidang (Donthu et al., 2021).

3. Visualisasi Data
Visualisasi hasil analisis dilakukan dalam tiga bentuk utama, yaitu *network visualization*, *overlay visualization*, dan *density visualization*. *Network visualization* digunakan untuk menunjukkan hubungan antar elemen dalam bentuk klaster penelitian. *Overlay visualization* digunakan untuk menganalisis

perkembangan topik berdasarkan waktu publikasi, sedangkan *density visualization* digunakan untuk mengidentifikasi area penelitian yang paling dominan dan intensif dalam bidang autentikasi berbasis matematika (Ramadani & Erwina, 2025).

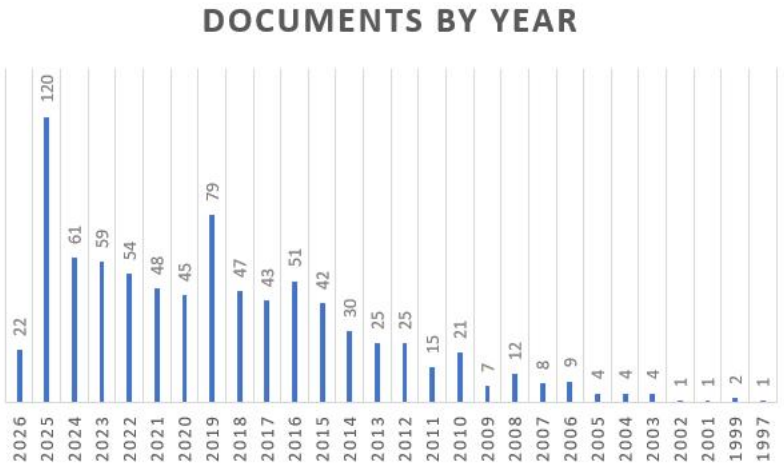
4. Interpretasi Hasil
   Hasil visualisasi yang diperoleh kemudian dianalisis secara deskriptif dan interpretatif untuk mengidentifikasi pola perkembangan penelitian, hubungan antar topik, kontribusi negara dan institusi, serta peluang penelitian yang masih terbuka. Interpretasi ini digunakan untuk menyusun rekomendasi arah penelitian di masa depan terkait pengembangan metode autentikasi berbasis matematika pada keamanan aplikasi mobile.

3. Hasil dan Pembahasan

3.1 Trend Publikasi Global

3.1.1 Jumlah Publikasi

Berdasarkan hasil pencarian dari database Scopus, dengan menggunakan kriteria pencarian sebagaimana dijelaskan dalam metode penelitian, diperoleh total sebanyak 840 dokumen ilmiah yang relevan. Pencarian ini menggunakan kombinasi kata kunci: *("mobile application" OR mobile) AND ("user authentication" OR authentication) AND ("cryptographic authentication" OR "biometric authentication")* yang merupakan representasi dari topik-topik utama dalam bidang keamanan aplikasi mobile berbasis metode autentikasi dan pendekatan kriptografi (matematika).



Suber: Database Scopus

Gambar 4. Pertumbuhan Jumlah publikasi Ilmiah Per Tahun

Berdasarkan hasil pencarian pada basis data Scopus menggunakan kriteria yang telah dijelaskan pada bagian metode penelitian, diperoleh sebanyak 840 dokumen ilmiah yang relevan dengan topik metode authentication berbasis matematika pada keamanan aplikasi mobile. Publikasi yang dianalisis mencakup periode 1997–2026 dan menunjukkan perkembangan yang dinamis dari waktu ke waktu.

Pada periode awal (1997–2005), jumlah publikasi masih relatif rendah, yaitu berkisar antara 1–4 dokumen per tahun. Kondisi ini menunjukkan bahwa penelitian mengenai autentikasi mobile masih berada pada tahap eksplorasi awal, seiring dengan masih terbatasnya penggunaan perangkat mobile dan layanan digital berbasis internet. Memasuki periode 2006–2013, jumlah publikasi mulai meningkat secara bertahap hingga mencapai 25 dokumen per tahun. Peningkatan ini berkaitan dengan berkembangnya teknologi *smartphone*, meningkatnya penggunaan layanan *mobile banking*, serta kebutuhan akan mekanisme autentikasi yang lebih aman dibandingkan sistem berbasis kata sandi konvensional.

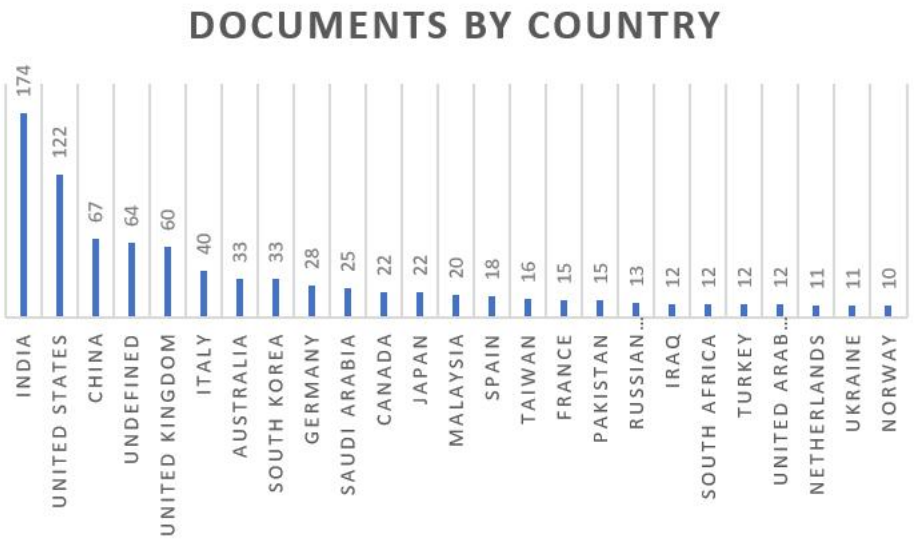
Tren peningkatan yang lebih signifikan terlihat pada periode 2014–2020 dengan jumlah publikasi berkisar antara 30–79 dokumen per tahun. Lonjakan publikasi pada periode ini dapat dikaitkan dengan beberapa perkembangan penting dalam bidang keamanan digital. Pertama, meningkatnya adopsi autentikasi biometrik pada perangkat mobile modern, khususnya setelah diperkenalkannya teknologi Face ID dan pengembangan sistem pengenalan biometrik yang semakin akurat. Kedua, implementasi regulasi perlindungan data seperti *General Data Protection Regulation* (GDPR) yang mulai berlaku di Uni Eropa pada tahun 2018 mendorong peningkatan perhatian terhadap keamanan identitas digital dan perlindungan data pengguna. Ketiga, berkembangnya teknologi *machine learning* dan *artificial intelligence* yang mulai banyak diterapkan pada sistem autentikasi adaptif dan *continuous authentication*. Faktor-faktor tersebut berkontribusi terhadap meningkatnya minat penelitian pada bidang autentikasi berbasis matematika.

Puncak sementara terjadi pada tahun 2019 dengan 79 publikasi. Namun demikian, jumlah publikasi mengalami penurunan menjadi 48 dokumen pada tahun 2021. Penurunan ini kemungkinan dipengaruhi oleh dampak global pandemi COVID-19 yang mengganggu aktivitas penelitian, kolaborasi internasional, serta proses publikasi ilmiah pada berbagai bidang. Selain itu, sebagian penelitian keamanan siber pada periode tersebut juga mengalami pergeseran fokus menuju isu keamanan infrastruktur digital, layanan daring, dan sistem kerja jarak jauh yang berkembang pesat selama masa pandemi.

Meskipun terjadi penurunan sementara, tren publikasi kembali meningkat secara signifikan setelah tahun 2021 hingga mencapai puncaknya pada tahun 2025 dengan 120 publikasi. Kondisi ini menunjukkan bahwa autentikasi berbasis matematika tetap menjadi salah satu topik penting dalam keamanan aplikasi *mobile*. Peningkatan tersebut juga dapat dikaitkan dengan berkembangnya penelitian mengenai post-quantum *cryptography*, *zero-knowledge proof, federated identity management*, serta integrasi kecerdasan buatan dalam sistem autentikasi *modern*. Dengan demikian, hasil analisis menunjukkan adanya korelasi positif antara perkembangan teknologi keamanan digital dan peningkatan jumlah publikasi ilmiah pada bidang autentikasi berbasis matematika.

Sementara itu, jumlah publikasi pada tahun 2026 tercatat sebanyak 22 dokumen. Nilai tersebut belum mencerminkan jumlah publikasi tahunan secara keseluruhan karena proses pengumpulan data dilakukan ketika tahun 2026 masih berlangsung sehingga masih dimungkinkan terjadi peningkatan jumlah dokumen hingga akhir tahun.

3.1.2 Kontribusi Negara



Suber: Database Scopus

Gambar 5. Grafik Kontribusi Negara

Grafik kontribusi negara menunjukkan bahwa India, United States, dan China merupakan kontributor utama dalam publikasi ilmiah terkait metode *authentication* berbasis matematika pada keamanan aplikasi *mobile*. India menempati posisi pertama dengan total 174 publikasi, diikuti oleh United States sebanyak 122 publikasi, serta China dengan 67 publikasi. Dominasi ketiga negara ini mencerminkan tingginya aktivitas riset di bidang keamanan siber dan kriptografi, yang didukung oleh perkembangan teknologi serta meningkatnya kebutuhan akan sistem keamanan digital. Selain itu, terdapat kategori *Undefined* dengan jumlah 64 publikasi yang menunjukkan adanya data afiliasi yang tidak teridentifikasi secara spesifik. Negara lain seperti United Kingdom (60 publikasi), Italy (40 publikasi), serta Australia dan South Korea (masing-masing 33 publikasi) juga menunjukkan kontribusi yang signifikan, diikuti oleh Germany (28 publikasi) dan Saudi Arabia (25 publikasi) yang turut berperan dalam pengembangan penelitian pada bidang ini.

Dominasi India, United States, dan China tidak hanya mencerminkan tingginya jumlah publikasi ilmiah, tetapi juga menunjukkan kuatnya ekosistem penelitian dan inovasi pada bidang keamanan siber di negara-negara tersebut. Amerika Serikat didukung oleh investasi riset yang besar, keberadaan lembaga standardisasi seperti *National Institute of Standards and Technology* (NIST), serta kolaborasi yang erat antara perguruan tinggi, industri teknologi, dan lembaga pemerintah dalam pengembangan standar keamanan digital. China menunjukkan pertumbuhan yang pesat seiring meningkatnya investasi nasional pada kecerdasan buatan, keamanan informasi, dan transformasi digital. Sementara itu, India memiliki keunggulan pada sektor teknologi informasi dan pengembangan perangkat lunak yang mendorong tingginya produktivitas penelitian pada bidang autentikasi, kriptografi, dan keamanan aplikasi *mobile*. Temuan ini menunjukkan bahwa dukungan kebijakan nasional, investasi penelitian dan pengembangan (*research and development*), serta kapasitas sumber daya manusia menjadi faktor penting yang memengaruhi produktivitas publikasi suatu negara.

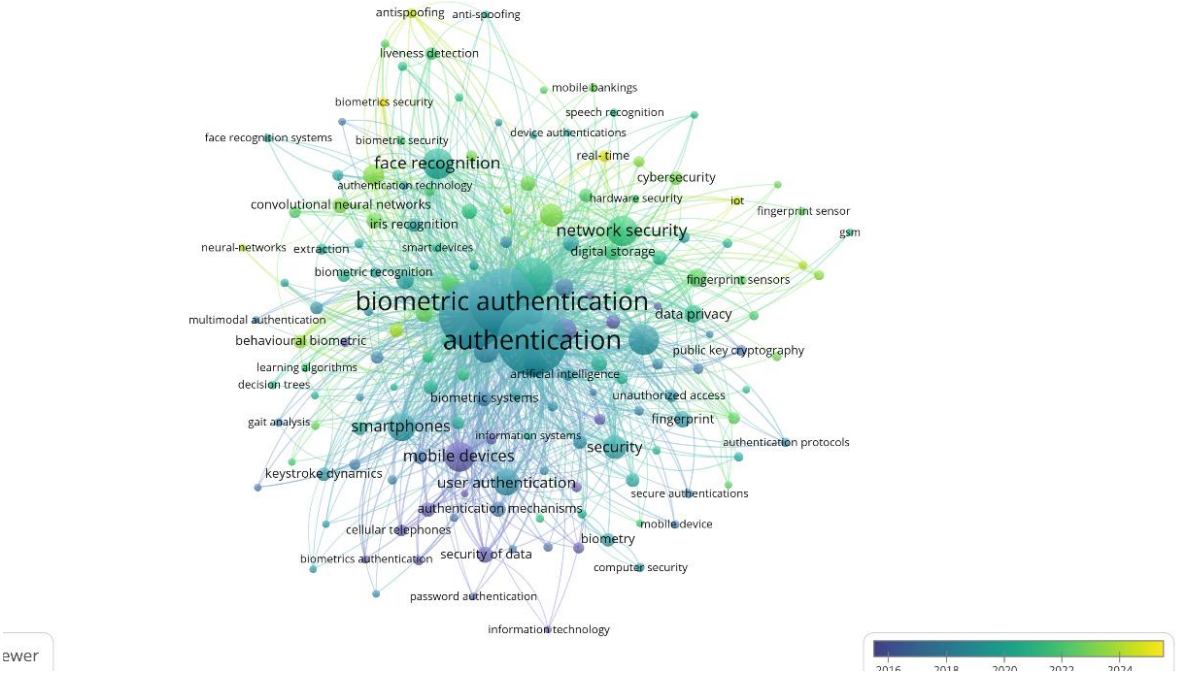
Menariknya, negara-negara ASEAN, termasuk Indonesia, belum termasuk dalam kelompok kontributor utama pada bidang ini. Kondisi tersebut menunjukkan bahwa penelitian autentikasi berbasis matematika masih didominasi oleh negara dengan kapasitas riset dan investasi teknologi yang tinggi. Di sisi lain, rendahnya kontribusi negara-negara ASEAN dapat dipandang sebagai peluang strategis untuk meningkatkan penelitian pada bidang keamanan siber, khususnya yang berkaitan dengan autentikasi biometrik, kriptografi, *machine learning*, dan kecerdasan buatan. Bagi Indonesia, temuan ini mengindikasikan perlunya peningkatan pendanaan riset, penguatan kolaborasi internasional, serta pengembangan pusat-pusat penelitian keamanan siber agar mampu meningkatkan kontribusi ilmiah dan daya saing penelitian pada tingkat global.

Dengan demikian, hasil analisis menunjukkan adanya hubungan yang konsisten antara perkembangan teknologi keamanan digital dan peningkatan jumlah publikasi ilmiah pada bidang autentikasi berbasis matematika. Lonjakan publikasi setelah tahun 2017 bertepatan dengan semakin luasnya penerapan autentikasi biometrik pada perangkat mobile, implementasi regulasi perlindungan data seperti *General Data Protection Regulation* (GDPR) pada tahun 2018, serta meningkatnya pemanfaatan kecerdasan buatan dalam sistem keamanan digital. Meskipun penelitian ini tidak melakukan analisis regresi statistik secara formal, pola pertumbuhan publikasi menunjukkan kecenderungan yang sejalan dengan berbagai *milestone* teknologi dan regulasi global yang memengaruhi perkembangan penelitian autentikasi modern.

Sementara itu, negara-negara dengan kontribusi menengah seperti Canada dan Japan (masing-masing 22 publikasi), Malaysia (20 publikasi), Spain (18 publikasi), Taiwan (16 publikasi), serta France dan Pakistan (masing-masing 15 publikasi) juga menunjukkan keterlibatan aktif dalam penelitian. Kontribusi juga datang dari negara seperti Russian Federation (13 publikasi), serta Iraq, South Africa, Turkey, dan United Arab Emirates (masing-masing 12 publikasi), yang menjadi batas akhir negara yang ditampilkan dalam grafik utama hingga Norway (10 publikasi). Adapun negara-negara lainnya yang tidak ditampilkan dalam grafik umumnya memiliki jumlah publikasi yang relatif kecil, yaitu kurang dari 10 dokumen, bahkan sebagian besar di bawah 5 publikasi. Meskipun demikian, keterlibatan negara-negara tersebut menunjukkan bahwa penelitian terkait autentikasi berbasis kriptografi telah menyebar secara global, meskipun masih didominasi oleh negara dengan kapasitas riset dan teknologi yang lebih maju.

3.2 Analisis Pemetaan Menggunakan VOSviewer

3.2.1 Co-Occurrence dengan Overlay Visualization



Sumber: Hasil Analisis Menggunakan VOSviewer

Gambar 6. Overlay Visualization

Tabel 1. Kategori Topik Berdasarkan Tahun

No	Tahun	Topik
1	**2016.0 – 2018.0**	*password authentication, user authentication, authentication mechanisms, security of data, information technology, computer security*
2	**2018.0 – 2020.0**	*mobile devices, smartphones, mobile security, biometric systems, biometric authentication, fingerprint, face recognition, network security, data privacy*
3	**2020.0 – 2022.0**	*artificial intelligence, neural networks, convolutional neural networks, biometric recognition, iris recognition, multimodal authentication, behavioural biometric*
4	**2022.0 – 2024.0**	*liveness detection, anti-spoofing, real-time authentication, cybersecurity, hardware security, IoT, public key cryptography, authentication protocols*

Gambar 6 menunjukkan hasil analisis *co-occurrence* menggunakan tampilan *overlay visualization* pada perangkat lunak VOSviewer. Pada visualisasi ini, warna node merepresentasikan nilai *average publication year* (APY) dari setiap kata kunci. Nilai APY dihitung oleh VOSviewer berdasarkan rata-rata tahun publikasi seluruh dokumen yang memuat kata kunci tertentu. Dengan demikian, semakin tinggi nilai APY maka semakin baru kecenderungan topik tersebut dalam literatur. Warna biru menunjukkan topik yang lebih awal muncul dalam publikasi, sedangkan warna hijau hingga kuning menunjukkan topik yang lebih baru dan sedang berkembang.

Untuk memudahkan interpretasi evolusi topik penelitian, kata kunci dikelompokkan ke dalam interval dua tahunan. Pemilihan interval dua tahun dilakukan karena rentang waktu tersebut cukup sensitif untuk menangkap perubahan tema penelitian tanpa menghasilkan fragmentasi yang terlalu rinci. Pendekatan ini

juga mempermudah identifikasi transisi topik dari satu fase perkembangan ke fase berikutnya berdasarkan distribusi nilai APY yang dihasilkan oleh VOSviewer.

Pada fase awal (2016–2018), penelitian didominasi oleh konsep dasar autentikasi dan keamanan sistem, seperti *password authentication*, *user authentication*, *authentication mechanisms*, *security of data*, dan *computer security*. Dominasi kata kunci tersebut menunjukkan bahwa fokus penelitian masih berada pada penguatan mekanisme autentikasi tradisional dan perlindungan akses pengguna. Secara bibliometrik, kata kunci-kata kunci tersebut memiliki nilai APY yang lebih rendah dibandingkan topik lainnya, sehingga muncul dalam warna yang lebih gelap pada visualisasi.

Memasuki periode 2018–2020, terjadi perluasan fokus penelitian menuju implementasi autentikasi pada perangkat *mobile*. Hal ini ditunjukkan oleh meningkatnya kemunculan kata kunci seperti *mobile devices*, *smartphones*, *biometric authentication*, *fingerprint*, *face recognition*, dan *data privacy*. Pergeseran tersebut sejalan dengan meningkatnya adopsi perangkat *mobile* yang dilengkapi sensor biometrik serta meningkatnya perhatian terhadap perlindungan data pribadi pengguna. Kemunculan kelompok kata kunci biometrik pada periode ini menunjukkan bahwa penelitian mulai berfokus pada peningkatan kenyamanan pengguna tanpa mengurangi tingkat keamanan sistem.

Pada periode 2020–2022, hasil *overlay visualization* menunjukkan meningkatnya keterkaitan antara autentikasi dan teknologi kecerdasan buatan. Kata kunci seperti *artificial intelligence*, *neural networks*, *convolutional neural networks*, *biometric recognition*, *iris recognition*, *multimodal authentication*, dan *behavioural biometric* memiliki nilai APY yang lebih tinggi dibandingkan topik sebelumnya. Temuan ini menunjukkan bahwa penelitian mulai memanfaatkan pendekatan *machine learning* dan *deep learning* untuk meningkatkan akurasi pengenalan identitas serta mengembangkan mekanisme autentikasi yang lebih adaptif terhadap perilaku pengguna.

Pada fase terbaru (2022–2024), muncul kelompok kata kunci seperti *liveness detection*, *anti-spoofing*, *real-time authentication*, *cybersecurity*, *hardware security*, *IoT*, *public key cryptography*, dan *authentication protocols*. Kemunculan kata kunci tersebut menunjukkan adanya pergeseran fokus dari sekadar identifikasi pengguna menuju pembangunan sistem autentikasi yang mampu menghadapi ancaman keamanan yang semakin kompleks. Topik *liveness detection* dan *anti-spoofing* berkembang sebagai respons terhadap meningkatnya risiko manipulasi biometrik dan serangan berbasis *deepfake*.

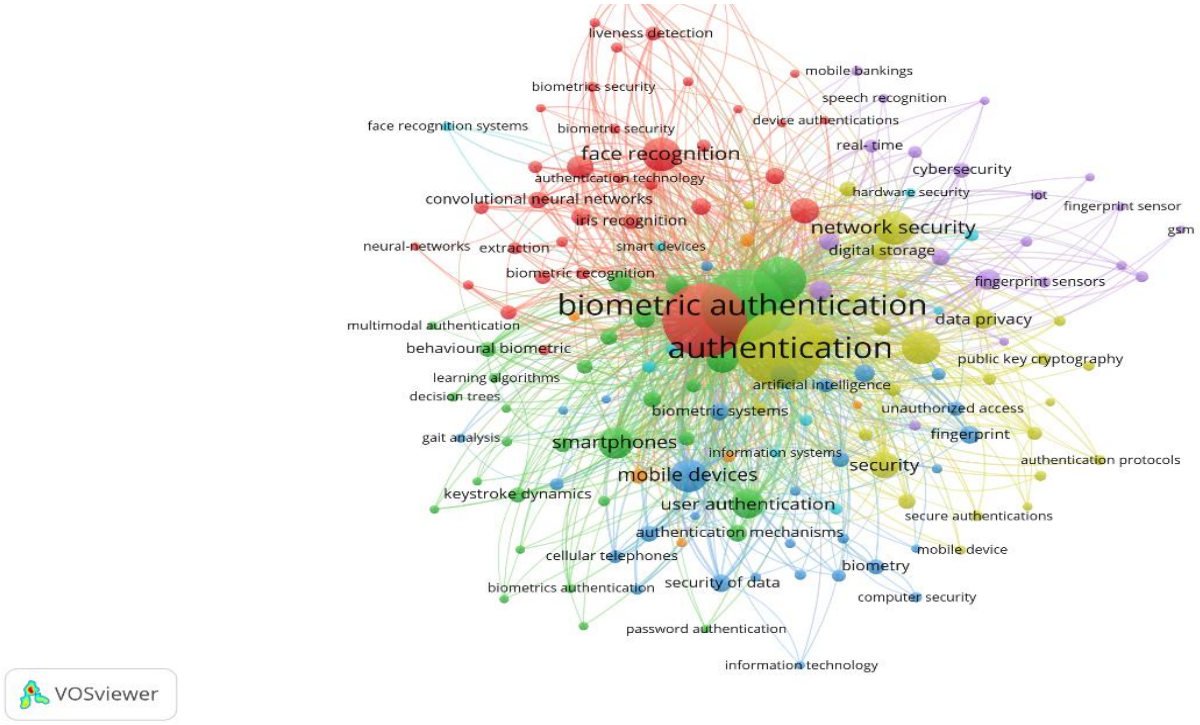
Menariknya, kata kunci *public key cryptography* dan *authentication protocols* memperoleh nilai APY yang relatif tinggi pada periode terbaru. Temuan ini tidak menunjukkan bahwa pendekatan kriptografi baru muncul atau kembali digunakan, karena kriptografi telah menjadi fondasi sistem autentikasi sejak periode awal. Sebaliknya, hasil bibliometrik mengindikasikan bahwa perhatian penelitian terhadap aspek kriptografi kembali meningkat dalam konteks tantangan keamanan modern. Dengan kata lain, terjadi peningkatan intensitas penelitian pada topik kriptografi tingkat lanjut, terutama yang berkaitan dengan keamanan IoT, protokol autentikasi modern, privasi data, serta kesiapan menghadapi ancaman komputasi kuantum. Hal ini terlihat dari posisi kata kunci kriptografi yang berada pada kelompok dengan nilai APY lebih tinggi dibandingkan kata kunci autentikasi tradisional.

Pola evolusi topik yang diperoleh juga memperkuat hasil penelitian (Kachbou et al., 2025) , yang menunjukkan bahwa visualisasi overlay efektif dalam menggambarkan perubahan fokus penelitian dari topik dasar menuju topik yang lebih mutakhir. Perbedaannya, penelitian ini secara khusus menunjukkan pergeseran dari autentikasi berbasis password menuju integrasi biometrik, artificial intelligence, dan public key cryptography pada keamanan aplikasi mobile.

Secara keseluruhan, hasil *overlay visualization* menunjukkan bahwa evolusi penelitian autentikasi pada aplikasi *mobile* bergerak dari pendekatan berbasis pengetahuan (*knowledge-based authentication*), menuju

autentikasi biometrik, kemudian berkembang ke arah integrasi kecerdasan buatan, dan pada fase terbaru mengarah pada penguatan keamanan melalui kombinasi biometrik, kecerdasan buatan, serta protokol kriptografi modern. Pola tersebut memperlihatkan bahwa perkembangan penelitian tidak menggantikan pendekatan sebelumnya, melainkan menunjukkan akumulasi dan integrasi berbagai metode untuk menjawab kebutuhan keamanan sistem *mobile* yang semakin kompleks.

3.2.2 Network Visualization



Sumber: Hasil Analisis Menggunakan VOSviewer

Gambar 7. Network visualization

Analisis *network visualization* dilakukan menggunakan metode *co-occurrence analysis* pada *author keywords* dengan bantuan perangkat lunak VOSviewer. Untuk meningkatkan relevansi jaringan dan mengurangi *noise* dari kata kunci yang jarang muncul, diterapkan *minimum occurrence threshold* sebesar 5 kemunculan. Dari keseluruhan kata kunci yang teridentifikasi pada data Scopus, sebanyak 160 kata kunci memenuhi ambang batas tersebut dan selanjutnya divisualisasikan ke dalam 7 cluster berdasarkan tingkat keterkaitannya. Hubungan antar kata kunci diukur menggunakan nilai *Total Link Strength* (TLS), yang merepresentasikan kekuatan hubungan *co-occurrence* dalam jaringan bibliometrik.

Berdasarkan hasil *network visualization*, struktur penelitian mengenai metode autentikasi pada keamanan aplikasi *mobile* menunjukkan keterkaitan yang kuat antara pendekatan biometrik, kecerdasan buatan, kriptografi, dan sistem komputasi terdistribusi. Meskipun terdiri atas berbagai istilah yang beragam, kata kunci dalam setiap *cluster* dapat direduksi menjadi tema-tema penelitian utama yang saling berhubungan.

Cluster 1 merupakan cluster dengan jumlah node terbanyak (35 kata kunci) dan didominasi oleh topik autentikasi biometrik berbasis kecerdasan buatan. Kata kunci seperti *face recognition*, *fingerprint recognition*, *iris recognition*, *deep learning*, *convolutional neural networks*, dan *neural networks* menunjukkan fokus penelitian pada peningkatan akurasi identifikasi biometrik menggunakan teknik pembelajaran mendalam. Kehadiran kata kunci *liveness detection*, *anti-spoofing*, dan *spoofing attacks* menunjukkan meningkatnya perhatian terhadap ketahanan sistem biometrik terhadap serangan manipulasi identitas.

Cluster 2 terdiri atas 31 kata kunci dan merepresentasikan autentikasi adaptif berbasis perilaku serta pembelajaran mesin. Kata kunci seperti *continuous authentication*, *behavioral biometrics*, *keystroke dynamics*, *touch dynamics*, *electrocardiography*, dan *machine learning* menunjukkan perkembangan penelitian menuju autentikasi dinamis yang mampu melakukan verifikasi identitas secara berkelanjutan berdasarkan pola perilaku pengguna.

Cluster 3 terdiri atas 30 kata kunci yang berfokus pada implementasi autentikasi dalam lingkungan komputasi *mobile*. Kehadiran kata kunci seperti *mobile applications*, *mobile devices*, *cloud computing*, *wearable technology*, *user identification*, dan *security of data* menunjukkan bahwa penelitian pada cluster ini menitikberatkan pada penerapan metode autentikasi pada berbagai platform dan perangkat bergerak.

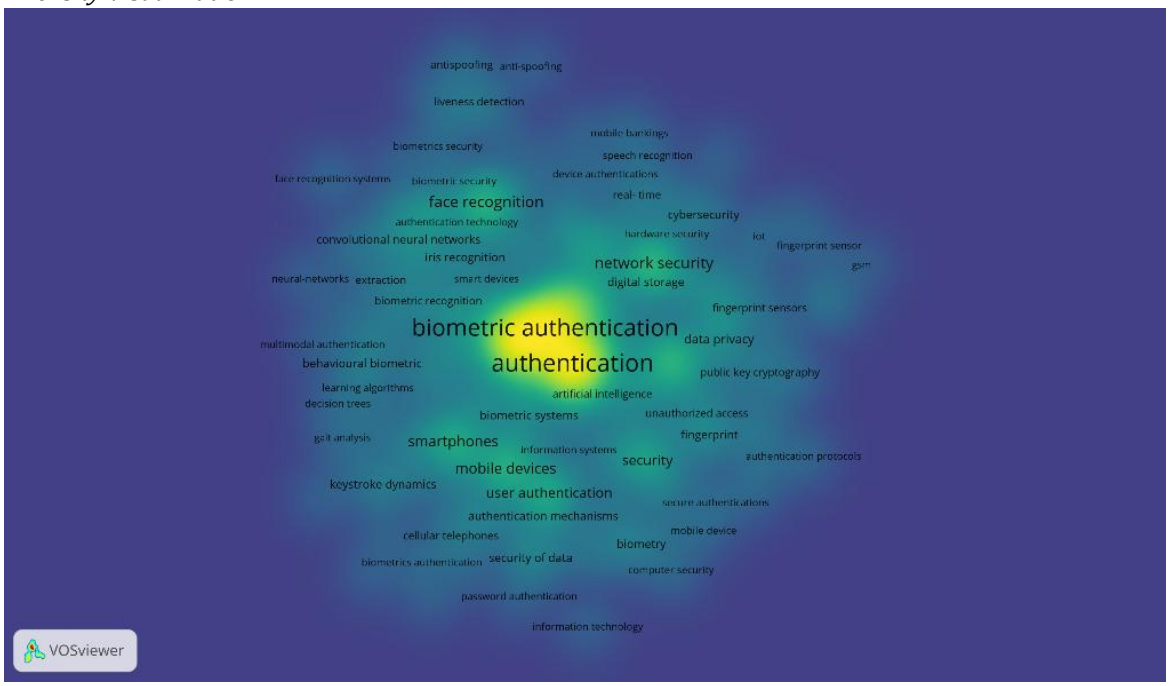
Cluster 4 terdiri atas 27 kata kunci dan menyoroti peran kriptografi sebagai fondasi autentikasi berbasis matematika. Kata kunci seperti *cryptography*, *public key cryptography*, *authentication protocols*, *mutual authentication*, *blockchain*, dan *privacy preserving* menunjukkan bahwa pendekatan matematis tetap menjadi komponen penting dalam menjamin keamanan, privasi, dan integritas sistem autentikasi modern.

Cluster 5 terdiri atas 20 kata kunci yang berkaitan dengan penerapan autentikasi pada ekosistem Internet of Things (IoT) dan perangkat cerdas. Kata kunci seperti *internet of things*, *smart devices*, *smart home*, *smart city*, *sensors*, dan *ubiquitous computing* menunjukkan bahwa penelitian autentikasi semakin berkembang pada lingkungan perangkat yang saling terhubung dan memiliki keterbatasan sumber daya komputasi.

Hasil ini juga konsisten dengan penelitian (Humaidi et al., 2025) yang menunjukkan bahwa penelitian keamanan informasi berkembang melalui keterkaitan beberapa tema utama, seperti keamanan jaringan, privasi data, dan mekanisme autentikasi. Namun demikian, penelitian ini memberikan cakupan yang lebih spesifik karena memetakan hubungan antara autentikasi biometrik, kecerdasan buatan, kriptografi, dan keamanan aplikasi mobile dalam satu jaringan bibliometrik.

Secara keseluruhan, hasil *network visualization* menunjukkan adanya konvergensi antara autentikasi biometrik, kecerdasan buatan, kriptografi, dan IoT dalam membentuk sistem autentikasi modern. Temuan ini mengindikasikan bahwa arah penelitian tidak lagi berfokus pada satu metode autentikasi tertentu, melainkan pada pengembangan sistem autentikasi hibrid yang mampu menggabungkan berbagai pendekatan untuk meningkatkan keamanan, adaptivitas, dan keandalan sistem.

3.2.3 Density Visualization



Sumber: Hasil Analisis Menggunakan VOSviewer
Gambar 8. Density visualization

Berdasarkan hasil analisis *co-occurrence* kata kunci menggunakan tampilan *density visualization* pada perangkat lunak *VOSviewer*, warna pada visualisasi merepresentasikan tingkat kepadatan kemunculan kata kunci dalam publikasi ilmiah. Warna kuning menunjukkan kepadatan tertinggi, diikuti oleh hijau sebagai kepadatan sedang, dan biru sebagai kepadatan rendah. Visualisasi ini memberikan gambaran mengenai fokus utama penelitian (*core research area*) serta area yang masih berkembang (*emerging research area*) dalam bidang autentikasi pada keamanan aplikasi *mobile*.

Hasil analisis menunjukkan bahwa kata kunci *authentication* dan *biometric authentication* berada pada area dengan intensitas warna paling tinggi, yang menandakan bahwa kedua topik tersebut merupakan pusat utama dalam struktur penelitian. Dominasi ini mencerminkan tingginya ketergantungan sistem keamanan *mobile* terhadap metode autentikasi berbasis biometrik, yang menawarkan kombinasi antara keamanan dan kemudahan penggunaan. Selain itu, keberadaan kata kunci seperti *mobile devices*, *smartphones*, *user authentication*, dan *security* di sekitar area pusat menunjukkan bahwa penelitian tidak hanya berfokus pada aspek konseptual, tetapi juga pada implementasi praktis dalam lingkungan perangkat *mobile*.

Lebih lanjut, kemunculan kata kunci seperti *network security*, *data privacy*, dan *public key cryptography* menunjukkan bahwa aspek perlindungan data dan keamanan jaringan tetap menjadi komponen penting dalam mendukung sistem autentikasi yang andal. Hal ini mengindikasikan bahwa meskipun biometrik mendominasi, pendekatan berbasis matematika, khususnya kriptografi, masih memiliki peran strategis dalam menjamin keamanan sistem secara menyeluruh.

Di sisi lain, kata kunci yang berada pada area dengan kepadatan lebih rendah, seperti *liveness detection*, *anti-spoofing*, *speech recognition*, dan *internet of things*, mengindikasikan bahwa topik-topik tersebut masih berada pada tahap pengembangan. Rendahnya kepadatan ini bukan menunjukkan kurangnya relevansi, melainkan menandakan adanya peluang penelitian yang signifikan. Hal ini terutama berkaitan dengan meningkatnya ancaman manipulasi biometrik, perkembangan teknologi kecerdasan buatan, serta integrasi autentikasi dalam ekosistem perangkat terhubung.

Secara keseluruhan, hasil *density visualization* menunjukkan bahwa penelitian dalam bidang autentikasi pada keamanan aplikasi *mobile* didominasi oleh pendekatan biometrik, namun mulai bergerak menuju integrasi yang lebih kompleks dengan aspek privasi, keamanan data, serta teknologi cerdas. Dengan demikian, area dengan kepadatan rendah dapat dipandang sebagai arah strategis untuk penelitian di masa depan, khususnya dalam pengembangan sistem autentikasi yang lebih adaptif, aman, dan tahan terhadap ancaman modern.

4. Kesimpulan

Penelitian ini berhasil memetakan perkembangan metode *authentication* berbasis matematika pada keamanan aplikasi *mobile* melalui analisis bibliometrik terhadap 840 publikasi yang terindeks Scopus periode 1997–2026. Hasil analisis menunjukkan bahwa penelitian mengalami pertumbuhan yang signifikan sejak tahun 2014, dengan evolusi topik dari autentikasi berbasis *password* menuju autentikasi biometrik, integrasi *artificial intelligence*, serta penguatan kriptografi dan protokol autentikasi modern. Selain itu, *network visualization* mengidentifikasi tujuh *cluster* utama yang menunjukkan keterkaitan antara biometrik, kecerdasan buatan, kriptografi, dan *Internet of Things* dalam pengembangan sistem autentikasi *mobile*.

Secara teoritis, penelitian ini memperkuat pemahaman mengenai evolusi pendekatan matematis dalam sistem autentikasi *mobile* serta menunjukkan keterkaitan antara kriptografi, biometrik, dan kecerdasan buatan sebagai fondasi autentikasi modern. Dibandingkan studi bibliometrik sebelumnya yang umumnya berfokus pada keamanan *mobile* atau kriptografi secara terpisah, penelitian ini memberikan pemetaan yang lebih terintegrasi dengan menghubungkan tren publikasi, struktur kolaborasi, dan evolusi topik dalam satu kerangka analisis. Secara praktis, hasil penelitian ini dapat menjadi referensi bagi peneliti dan pengembang sistem dalam mengidentifikasi teknologi autentikasi yang berkembang serta peluang penelitian yang masih terbuka.

Penelitian ini masih terbatas pada penggunaan basis data Scopus sehingga belum sepenuhnya merepresentasikan seluruh publikasi yang tersedia pada basis data lain. Oleh karena itu, penelitian selanjutnya disarankan untuk mengintegrasikan data dari Web of Science, IEEE Xplore, atau Dimensions serta mengombinasikan analisis bibliometrik dengan *systematic literature review* maupun evaluasi eksperimental. Topik seperti *anti-spoofing authentication*, autentikasi pada ekosistem IoT, *privacy-preserving authentication*, dan *post-quantum cryptography* merupakan area yang berpotensi menjadi fokus penelitian pada masa mendatang.

5. Referensi

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*, 285–296.

Gilbert, C., & Gilbert, M. A. (2025). Continuous User Authentication on Mobile Devices. *International Research Journal of Advanced Engineering and Science*, *10*(1), 158–173.

Hasan, S. S. U., Ghani, A., Daud, A., Akbar, H., & Khan, M. F. (2025). A Review on Secure Authentication Mechanisms for Mobile Security. In *Sensors* (Vol. 25, Number 3). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s25030700

Hasija, T., Ramkumar, K. R., Kaur, A., & Bali, M. S. (2025). Exploring the landscape of post quantum cryptography: a bibliometric analysis of emerging trends and research impact. *Journal of Big Data*, *12*(1). https://doi.org/10.1186/s40537-025-01269-5

Humaidi, N., Zainal, N., & Muhamat, A. A. (2025). Mapping the Landscape of Information Security Risk Management Research: A Bibliometric Analysis Using VOS Viewer and Power BI. *Journal of Information Assurance and Security*, *20*(2), 86–105. https://doi.org/10.2478/ias-2025-0006

Kachbou, Y., Mhammedi, M. A., Aichouch, I., Azzaoui, K., Touzani, R., & Hammouti, B. (2025). Bibliometric analysis of global research trends on UIZ using Scopus database and VOS viewer from 1989-2024. *J. Mater. Environ. Sci*, *2025*(5), 849–865. http://www.jmaterenvironsci.com

Korać, D., Damjanović, B., Simić, D., & Pu, C. (2025). Management of evaluation processes and creation of authentication metrics: Artificial intelligence-based fusion framework. *Information Processing & Management*, *62*(6), 104233. https://doi.org/https://doi.org/10.1016/j.ipm.2025.104233

Ramadani, T. A. S., & Erwina, W. (2025). Bibliometric analysis: Trends research application of information technology in university libraries. *Informatio: Journal of Library and Information Science*, *5*(3), 321–336. https://doi.org/10.24198/inf.v5i3.65182

Van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(2), 523–538.

Yeovandi, F., Sabariman, S., & Prasetyo, S. E. (2025). Evaluasi Keamanan Sistem Autentikasi Biometrik pada Smartphone dan Rekomendasi Implementasi Optimal. *JTIM : Jurnal Teknologi Informasi Dan Multimedia*. https://api.semanticscholar.org/CorpusID:275807995