KHAZANAH
Jurnal Pengembangan Kearsipan
Khazanah: Jurnal Pengembangan Kearsipan, 16(2), 203-220

Sistem Kriptografi pada Pengamanan Autentikasi Dokumen Elektronik: *Systematic Literature Review*

I N T I S A R I

Kebutuhan akan penjagaan kerahasiaan informasi dan keamanan autentikasi dokumen elektronik dirasa semakin meningkat. Penelitian ini bertujuan untuk mendeskripsikan bahwa konsep penyandian sistem kriptografi pada pengamanan autentikasi dokumen elektronik adalah menjamin keaslian, kerahasiaan, dan keamanan dokumen elektronik tersebut. Sistem kriptografi dapat menjaga keamanan yang sangat ketat karena tidak memungkinkan terjadinya penyadapan dan pengubahan data oleh pihak luar yang tidak sah. Penelitian menggunakan metode *systematic literature review* (SLR) pada sembilan artikel terseleksi dari database *Scopus* yang diterbitkan pada tahun 2018-2022, kemudian dianalisis bibliometrik menggunakan *VOSviewer* untuk mengidentifikasi peluang penelitian dalam topik sejenis. Berdasarkan hasil analisis terdapat sembilan artikel yang diseleksi ditemukan bahwa terdapat beberapa jenis sistem kriptografi yang digunakan untuk pengamanan kerahasiaan dan keaslian autentikasi dokumen elektronik di berbagai negara baru-baru ini yaitu *access control, blockchain, cloud computing, cryptography, digital signature, encryptiption and searchable encryption.* Berdasarkan tahun publikasi 2017-2022, negara yang sudah menerapkan sistem kriptografi pada pengamanan autentikasi dokumen elektronik adalah China, India, United States, Germany, Japan, Australia, Saudi Arabia, Canada, France, dan Russian. Hasil penelusuran menunjukkan penulis, institusi, dan negara mana saja yang melakukan penelitian mengenai penyandian sistem kriptografi untuk pengamanan autentikasi dokumen elektronik. Publikasi mengenai sistem kriptografi pada pengamanan dokumen elektronik cenderung mengalami peningkatan yang signifikan dari tahun 2018-2020.

KATA KUNCI

autentikasi,
dokumen elektronik,
enkripsi dan deskripsi,
sistem kriptografi, *VOSviewer*

A B S T R A C T

The need for maintaining the confidentiality of information and the security of electronic document authentication is felt to be increasing. This study aims to

KEY WORDS

authentication, cryptographic documents, electronic document, encryption and description, VOSviewer

PENULIS

Aisyah Romauli Harahap
Tamara Andriani Salim

Universitas Indonesia,
Jawa Barat, Indonesia
aisyah.romauli@ui.ac.id
tamaraas@ui.ac.id

describe that the concept of cryptographic system encryption in securing electronic document authentication is to guarantee the authenticity, confidentiality, and security of these electronic documents. The cryptographic system can maintain very tight security because it does not allow wiretapping and alteration of data by unauthorized outside parties. The study used the systematic literature review (SLR) method on nine selected articles from the Scopus database published in 2018-2022, then analyzed bibliometrics using VOSviewer to identify research opportunities on similar topics. Based on the results of the analysis of the nine articles selected, it was found that there are several types of cryptographic systems used to secure the confidentiality and authenticity of electronic document authentication in various countries recently, namely access control, blockchain, cloud computing, cryptography, digital signature, encryption and searchable encryption. Based on the 2017-2022 publication year, countries that have implemented a cryptographic system to secure electronic document authentication are China, India, United States, Germany, Japan, Australia, Saudi Arabia, Canada, France, and Russia. The search results show which authors, institutions and countries have conducted research on cryptographic system encryption for securing electronic document authentication. Publications regarding cryptographic systems for securing electronic documents tend to experience a significant increase from 2018-2020.

PENGANTAR

Latar Belakang Masalah

Dewasa ini pengguna internet dan jaringan komputer yang digunakan untuk saling mengirim dan menerima data semakin meningkat. Oleh karena itu, pengamanan keaslian, kerahasiaan, dan keamanan dokumen elektronik pada jaringan komunikasi antar data dengan penyandian sistem kriptografi menjadi penting. Bidang kearsipan sebaiknya mengubah sistem arsip manual ke sistem yang terkomputerisasi dalam era teknologi dan informasi. Agar dapat terjaga keamanan dan kerahasiaannya, perlu dilakukan pengamanan yang ketat pada dokumen elektronik yang telah disimpan. Salah satu caranya adalah dengan melakukan proses penyandian (*enkripsi*) informasi yang akan diarsipkan ke dalam berbagai *file* data disesuaikan dengan kebutuhan (*deskripsi*).

Pengamanan ketat perlu dilakukan karena banyaknya dokumen elektronik yang bersifat rahasia. Pengamanan akan menjaga dokumen elektronik agar tidak bisa diubah oleh pihak luar (yang tidak berhak), penghindaran dari kebobolan, pencegahan pencurian data, yang paling penting menghindari *carder, hacker, cracker,* dan lain-lain. Pengamanan dokumen elektronik menggunakan penyandian sistem kriptografi dengan bertujuan untuk menjaga autentikasi dokumen elektronik.

Sistem kriptografi merupakan teknik penyandian untuk keselamatan dan keamanan data *file* yang berupa arsip, dokumen, gambar, video, maupun audio. Untuk mengatasi permasalahan pengamanan dalam hal peningkatan tindak pencurian serta publikasi yang dilakukan oleh media lainnya, maka digunakan penyandian sistem kriptografi (Rosmasari, 2018: 172-181). Karena tingginya tingkat transaksi pengaksesan data, dikhawatirkan muncul kesalahan sistem. Banyak pengguna internet dengan bebas mengakses kebutuhan informasi yang positif maupun negatif sehingga perlu menjaga keamanan data tersebut. Sistem kriptografi merupakan solusi alternatif yang dapat digunakan untuk pengamanan data. Beberapa penelitian yang ditemukan menunjukkan pentingnya pengamanan data menggunakan penyandian sistem kriptografi.

Sistem penyandian kriptografi dikenal menggunakan dua metode, yaitu kunci publik dan konvensional. Dalam proses penyandian sistem kriptografi kunci publik diperlukan dua buah kunci penyandian yaitu enkripsi data yang tidak dirahasiakan (kunci publik) dan deskripsi data yang harus dijaga kerahasiaannya (kunci privat). Proses penyandian sistem kriptografi dilakukan dengan mengubah bentuk *plaintext* ke *chipertext*. Begitu juga sebaliknya, diperlukan sebuah kunci penyandian dengan kunci yang sama dan seharusnya dijaga ketat kerahasiaan.

Dokumen elektronik merupakan aset yang penting dan sumber informasi dalam bentuk elektronik yang diperlukan oleh suatu organisasi, instansi, perkantoran, negara maupun individu. Sebuah dokumen jika tidak dijaga dengan baik, kemungkinan bisa menyebabkan terjadinya kehilangan atau pencurian data di masa yang akan datang. Seiring perkembangannya, pemalsuan dokumen dapat dengan mudah dikerjakan oleh pihak-pihak yang tidak mempunyai kepentingan dan akses masuk. Bentuk pemalsuan dokumen baru menggunakan beberapa desain dan tampilan yang sama persis dengan dokumen aslinya. Menghindari hal tersebut, dibutuhkan penyandian sistem kriptografi untuk pengamanan autentikasi dokumen elektronik agar dapat menjaga keaslian, kerahasiaan, dan keamanan data.

Rumusan Masalah

Berdasarkan gambaran umum mengenai sistem kriptografi, maka peneliti bermaksud mengkaji bagaimana sistem kriptografi pada pengamanan autentikasi dokumen elektronik di berbagai negara di belahan dunia melalui *study literature review* (SLR) pada artikel terindeks *Scopus*. Peneliti menggunakan metode analisis bibliometrik dengan bantuan aplikasi *VOSviewer* untuk mengetahui sistem kriptografi dihubungkan dengan penyandian enkripsi dan deskripsi pada pengamanan autentikasi dokumen elektronik. Masih sangat sedikit penelitian atau literatur yang mengungkapkan topik bahasan sistem kriptografi pada pengamanan dokumen elektronik. Pada analisis ini, peneliti menggunakan beberapa jurnal penelitian elektronik (*e-journal*) dengan rentang waktu penelitian dari tahun 2017 hingga tahun 2022. Dari rumusan permasalahan tersebut peneliti berharap dapat melihat performa dari sistem kriptografi di berbagai negara sehingga menghasilkan penilaian akan pembelajaran dan penerapannya di Indonesia.

Tujuan Penelitian

Penelitian ini bertujuan untuk mengetahui bagaimana sistem kriptografi untuk keamanan autentikasi dokumen elektronik digunakan di berbagai negara. Dengan demikian agar dapat diketahui kemungkinan penerapannya pada bidang pengarsipan di Indonesia sehingga keterjangkauan kerja keamanan dokumen elektronik dapat terlihat transparan.

Metode Penelitian

Metode penelitian yang diterapkan dalam penelitian ini adalah metode literatur *review* secara sistematis untuk menelaah kajian pustaka. Untuk menganalisis literatur, peneliti menggunakan aplikasi *VOSviewer*. *VOSviewer* digunakan untuk memvisualisasikan bibliografi atau data set yang berisi *field bibliography* (judul, pengarang, penulis, nama jurnal, dan sebagainya). *VOSviewer* juga digunakan untuk analisis bibliometrik, mencari topik yang masih ada peluangnya untuk diteliti, mencari referensi lain yang paling banyak digunakan di bidang tertentu. SLR merupakan sebuah teknik analisis sistematis pustaka yang sering diterapkan oleh para peneliti sebelumnya (Chan dkk, 2016; Chan & Owusu, 2017; Hansen, 2020: 463–474).

SLR yang digunakan dalam penelitian ini terdiri dari beberapa proses, yaitu: a) *planning*, tahapan perencanaan untuk melihat aturan terstruktur yang didasari pada konteks ini, aturan peninjauan yang ditentukan, pembuatan pertanyaan penelitian, dan penyeleksian database jurnal elektronik yang akan

digunakan dengan tujuan agar menemukan jawaban dari pertanyaan penelitian, b) *conducting*, tahapan pelaksanaan yang dilalui dengan strategi pencarian dan ekstraksi data untuk mengategorikan item data sebagai output menggunakan kata kunci, melakukan inklusi dan eksklusi data yang telah ditemukan, c) *reporting*, tahapan pelaporan yang menyimpulkan pembahasan dan hasil temuannya dan memberikan penilaian atas hasil penelitian tersebut.

Tahap-tahap dalam melakukan proses pengumpulan hasil pencarian data, kemudian dianalisis oleh aplikasi *VOSviewer* adalah sebagai berikut.

1. Melakukan seleksi dan penyaringan artikel ilmiah yang relevan, yaitu penelitian yang dihimpun berdasarkan tahun terbit publikasi di tahun 2017 hingga tahun 2022 memakai mesin pencarian informasi artikel ilmiah terindeks *Scopus*. Tahun 2017 dipilih sebagai rentang awal tahun karena sistem kriptografi mulai diperkenalkan, digunakan, dan dipromosikan untuk keamanan penyandian dokumen elektronik. Proses berikutnya pada tahapan ini, yakni a) tahapan pertama, peneliti membuat batasan kriteria kata kunci pencarian, b) tahapan kedua, melakukan filterisasi artikel dengan membuat batasan menggunakan artikel yang bersumber dari jurnal dan prosiding dan hanya menggunakan artikel berbahasa inggris, dan c) tahapan ketiga, peneliti melakukan impor hasil dari tahapan kedua dalam format PDF. Tinjauan ulang dilakukan secara manual, yaitu memeriksa dan membaca abstrak, kata kunci penulis, kata kunci indeks, dan kutipan untuk menentukan pengecualian dari daftar hasil pencarian.
2. Pada tahap ini peneliti melakukan analisis artikel. Hasilnya adalah data dalam bentuk gambar yang dapat menunjukkan peta dan tema-tema berwarna yang muncul berdasarkan pembuatan kategori di dalam aplikasi *VOSviewer. VOSviewer* berisikan visualisasi data, yaitu a) tergambarnya besar kecil garis yang menghubungkan serta terdapat lingkaran. Hal ini terlihat dengan besar kecilnya angka hasil *VOSviewer,* b) kemudian terlihat beberapa angka ini terbagi menjadi bentuk *link* (jejaring yang dimiliki) dengan menghitung kekuatan link (perhitungan berdasarkan

full atau *fractional counting*) dengan banyaknya kemunculan hasil informasi.

Setelah tahapan di atas, ada beberapa cakupan tahapan jenis yang dianalisis, yakni: a) visualisasi dokumen dengan mengamati *citation*. Pengujian atau pengamatan terhadap dokumen akan dihubungkan dengan dokumen lainnya jika penulis artikel menyitir artikel lainnya yang sama-sama akan diamati. Analisis ini digunakan untuk memperlihatkan sitasi antar dokumen, b) *bibliography coupling*, pengujian artikel dengan visualisasi dokumen dan digambarkannya *network* apabila memiliki referensi yang sama. Analisis ini dilakukan untuk menunjukkan kedekatan-kedekatan kajian-kajian antar dokumen, c) *co-authorship*, melakukan analisis kolaborasi antar penulis dengan penulis lainnya. Analisis hasil visualisasi berdasarkan nama penulis, institusi atau organisasi penulis, ataupun negara asal penulis. Adapun hasil dari output *VOSviewer* mempunyai tiga tampilan, yaitu *density visualization*, *network visualization*, dan *overlay visualization.*

Beberapa proses metode SLR, sebagai berikut.

Planning

Pada tahapan *planning*, *research question* bertujuan agar penelitian ini dapat terstruktur, dengan membuat penentuan pertanyaan dan batasan pada penelitian. Berikut batasan-batasan dalam *research question*, antara lain: a) karakteristik *population*, mencakup sistem kriptografi pada pengamanan autentikasi dokumen elektronik. b) karakteristik *intervention*, mencakup artikel yang mengkaji sistem kriptografi pada pengamanan dokumen elektronik. c) karakteristik *comparison,* dengan cakupan tidak ditentukan. d) karakteristik *outcomes*, dengan cakupan model penerapan sistem kriptografi yang paling banyak digunakan dan memperoleh hasil atau kesimpulan yang positif (*construct*). e) karakteristik *context*, dengan cakupan melakukan review terhadap semua literatur terkait sistem kriptografi.

Berdasarkan kategorisasi dan Batasan tersebut, dibuat dua pertanyaan penelitian (RQ), yaitu:

1. RQ1: Berapa banyak *item* dan *cluster* yang ditemukan pada *VOSviewer* mengenai sistem kriptografi pada pengamanan autentikasi dokumen elektronik?
2. RQ2: Berapa banyak penelitian yang relevan dengan sistem kriptografi pada pengamanan autentikasi dokumen elektronik?

Conducting

Pada tahapan ini menggunakan pendekatan PRISMA (P*referred Reporting Items for Systematic Reviews and Meta Analyses*). Menggunakan kriteria *boolean OR and AND*, yaitu a)

population [Penerapan penyandian sistem kriptografi OR Implementasi penyandian sistem kriptografi AND]. b) *intervention* [Autentikasi dokumen elektronik OR Autentikasi arsip elektronik AND]. dan c) *method* [Tren OR Perkembangan AND]

Literature Resources

Scopus (www.scopus.com) adalah sebuah database jurnal online yang terpublikasi internasional yang berisikan kumpulan-kumpulan informasi dari berbagai bidang studi. Kemudian dilakukan *selection* berdasarkan tahun terbitan publikasi dari tahun 2017 hingga tahun 2022.

Inclusion and Exclusion Criteria

Inklusi dan eksklusi ini digunakan untuk menyeleksi berdasarkan kriteria dan memfokuskan pada artikel jurnal online yang sesuai dengan kebutuhan peneliti. Point dari kriteria-kriteria inklusi dan eksklusi yang diberikan, kemudian akan dijabarkan sebagai berikut:

a. *Inclusion Criteria* (hanya artikel yang menggunakan metode penerapan penyandian sistem kriptografi, fokus artikel pengkajian penerapan penyandian sistem kriptografi, artikel dipublikasikan dari tahun 2017-tahun 2022, dan semua publikasi artikel jurnal)
b. *Exclusion Criteria* (artikel yang tidak menggunakan metode penerapan penyandian sistem kriptografi, tidak fokus artikel pengkajian penerapan penyandian sistem kriptografi, artikel tidak dipublikasikan dari tahun 2017-tahun 2022, dan selain publikasi artikel jurnal (buku, disertasi, prosiding, skripsi, tesis)

Reporting

Penilaian kualitas hasil penelusuran bertujuan untuk mengevaluasi kualitas artikel jurnal dan kebermanfaatan data yang didapatkan. Adapun pertanyaan yang akan mendukung untuk penilaian hasil penelusuran. Setiap pertanyaan memiliki tiga pilihan jawaban, yaitu: Ya = 1; Ragu-ragu = 0.5; Tidak = 0. Berikut penilaian kualitas penelusuran, yaitu: a) Q1: Apakah ada pembahasan penelitian tentang sistem kriptografi?; b) Q2: Apakah ada manfaat dari penelitian penerapan sistem kriptografi?; c) Q3: Apakah penelitian ini akan membahas manfaat dan tantangan dari penerapan sistem kriptografi?

Kerangka Pemikiran

Peraturan Kepala Arsip Nasional Republik Indonesia Nomor 20 Tahun 2011 tentang Pedoman Autentikasi Arsip Elektronik menyatakan bahwa autentikasi merupakan proses dari pemberian tanda dan/atau tanda lain sesuai dengan perkembangan teknologi yang menunjukkan bahwasanya arsip yang diautentikasi adalah asli atau sesuai

dengan asli. Proses autentikasi yang harus diperhatikan, antara lain:

a) kebenaran, keabsahan atau validitas identitas oleh pihak dari berasal yang mempunyai nilai informasi atau dokumen elektronik, dan pihak pengirim-penerima;
b) keabsahan wewenang dari pihak yang menciptakan, mengirimkan, dan menerima informasi atau dokumen elektronik tersebut;
c) keabsahan validitas dari peralatan (yang secara lebih luas, sistem informasi, komunikasi, termasuk sistem elektronik) yang digunakan untuk penciptaan, pengiriman, penyimpanan, penerimaan informasi atau dokumen elektronik tersebut;
d) penjaminan keutuhan ataupun integritas informasi atau dokumen elektronik tersebut berarti hal memang sah dan benar atau unik, yang hanya memang dimuat di awal pada keperluan yang ditujukan tanpa adanya pengubahan secara paksa tanpa hak yang ada.

Aspek yang diperhatikan dalam autentikasi dokumen elektronik, antara lain a) *integrity*, aspek yang mempunyai hubungan dengan pembuktian kebenaran ada dokumen elektronik, sehingga isi dari dalam informasi masih mempunyai pertanggungjawaban penilaian ada kebenaran, b) *usability*, aspek penglihatan nilai guna dari isi informasi yang terkait dengan dokumen yang diciptakan, dan mengandung catatan yang berawal dalam suatu kegiatan yang masih berlangsung. c) *reliability*, dokumen elektronik hasil dari alih media yang tidak dapat terlepas dari bentuk yang asli, yang akan dijadikan penunjang dari sebuah keautentikan dokumen elektronik tersebut.

Pemetaan penyandian sistem kriptografi terdiri dari beberapa bagian, yaitu

1) *plaintext* adalah penciptaan kode penyandian teks yang asli dapat terbacakan dan memiliki arti tertentu. 2) *enkripsi* adalah proses kode penyandian (*encode*) dengan menggunakan kode kuncian atau parameter tertentu. 3) *ciphertext* adalah hasil dari sebuah proses penyandian enkripsi, yang berisikan informasi yang tidak memiliki terjemahan. 4) *deskripsi* adalah sebuah proses yang dipergunakan untuk temu kembali(*decode*) dari sebuah *ciphertext* ke sebuah *plaintext.*

Beberapa aspek yang terdapat di penyandian sistem kriptografi, antara lain: a) *confidentiality,* aspek penjagaan agar pesan informasi tidak dapat terbaca oleh pihak luar (pihak yang tidak berhak akses membaca atau melihat pesan), b) *data integrity*, aspek penjaminan, menjamin pesan yang masih asli ataupun belum

pernah dimanipulasi selama proses pengirimannya, c) *authentication*, aspek identifikasi, mengidentifikasi kebenaran nilai asli antara pihak-pihak yang saling berkomunikasi (*user authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*), d) *non-repudiation,* aspek penyangkalan, tujuannya untuk pencegahan entitas, dengan tujuan pengirim pesan penyangkalan melakukan pengiriman pesan dan penerima pesan penyangkalan telah menerima pesan tersebut, e) *authority*, aspek modifikasi, untuk akses memodifikasi pesan oleh pihak yang punya berkas, f) *privacy*, aspek tertutup dan tidak bisa bebas akses, g) *availability*, aspek ketersediaan akses terbuka ketika dibutuhkan. Apabila sistem informasi suatu database tiba-tiba diserang virus atau *hack,* otomatis keamanannya bergerak untuk menghambat, h) *access control,* aspek akses kontrol untuk pengaturan ketika akan menuju suatu database sumber informasi yang berkaitan dengan *privacy* dan *authentication*.

PEMBAHASAN

Hasil Pencarian

Hasil penelusuran *Scopus* terdapat pada tabel 5 dan gambar 2. Proses penyeleksian artikel dibedakan menjadi tiga tahapan, antara lain: a) tahapan kesatu, tahapan dengan kriteria penelusuran dengan *keyword* yang ditetapkan terdapat sebanyak 722 artikel jurnal, b) tahapan kedua, dibagi lagi ke beberapa bagian yakni, 1) penyertaan dengan didasari jenis artikel ilmiahnya (hanya jurnal dan prosiding) terdapat sebanyak 267 artikel jurnal, 2) penyertaan dan pengecualian berdasarkan bahasa yang ditentukan (hanya bahasa inggris) terdapat sebanyak 244 artikel jurnal, dan 3) dikecualikan berdasarkan tahun terbit (artikel tidak terkait dengan bidang studi dikecualikan) terdapat sebanyak 183 artikel jurnal, c) tahapan ketiga, pengecualian didasari abstrak dan kata kunci (artikel tidak terkait dengan abstrak dan kata kunci akan dikecualikan) terdapat sebanyak sembilan artikel yang selanjutnya akan diulas lebih lanjut dalam penelitian ini.

Pembahasan

Melalui metode SLR yang sudah disesuaikan dengan kriteria tertentu, literatur kemudian di *review* dan selanjutnya identifikasi *research question* dengan data temuan yang dihimpun.

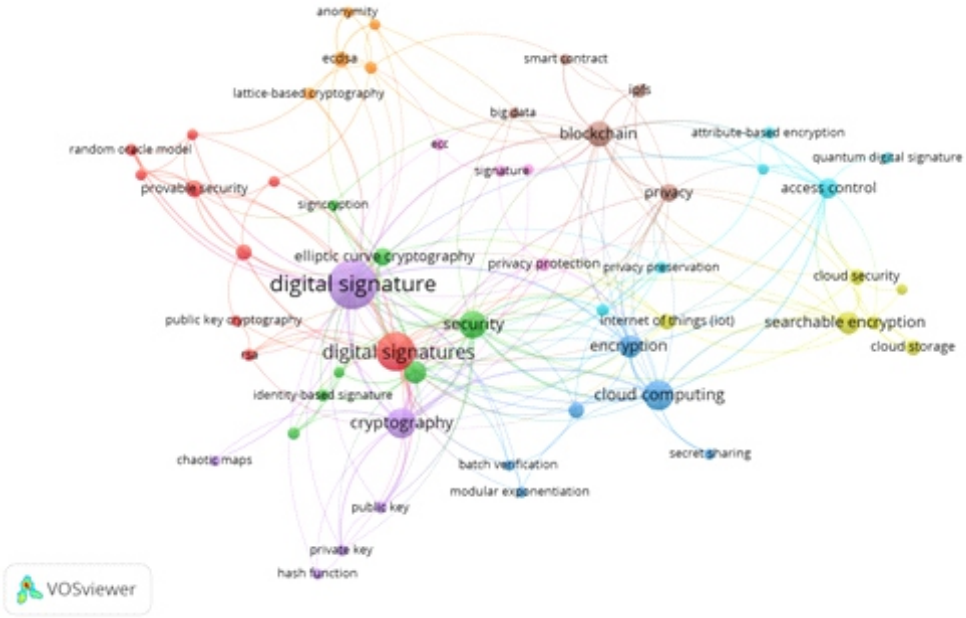
Rq1: Berapa banyak *item* dan *cluster* yang ditemukan pada *VOSviewer* mengenai penelitian tentang sistem kriptografi pada pengamanan autentikasi dokumen elektronik?

Tabel 1
Criteria-based stages Scopus

Stages	***Inclusion/Exclusion***	***Description***	***Search Criteria***	***Results***
Kesatu	Kriteria Pencarian	Kata kunci	TITLE-ABS-KEY (cryptographic AND systems AND document AND electronic)	722
Kedua	Penyertaan berdasarkan jenis artikel ilmiah	Hanya menyertakan artikel dari jurnal dan prosiding	AND (LIMID-TO (DOCTYPE< "ar"))	267
	Penyertaan dan pengecualian berdasarkan bahasa	Hanya artikel ilmiah yang berbahasa Inggris yang dicantumkan selainnya dikecualikan	AND (LIMIT-TO (LANGUAGE< "English"))	244
	Pengecualian berdasarkan tahun terbit	Artikel tidak terkait dengan tahun terbit akan dikecualikan	AND (EXCLUDE (PUB YEAR, 2022) OR EXCLUDE (PUB YEAR, 2021) OR EXCLUDE (PUB YEAR, 2019) OR EXCLUDE (PUB YEAR, 2018) OR EXCLUDE (PUB YEAR, 2017))	183
Ketiga	Pengecualian berdasarkan abstrak dan kata kunci	Artikel tidak terkait dengan abstrak dan kata kunci akan dikecualikan	Data akan diunduh format CSV dan PDF RIS Abstrak dibacakan tahap demi tahap untuk kriteria pencarian	9

Sumber: *Research Data* 2022

a. Network Visualization



Gambar 1
Tampilan Peta *Network Visualization*
Sumber: *VOSViewer* 2022

Berdasarkan hasil peta *network visualization*, diketahui bahwa terdapat keterhubungan antara tema sistem kriptografi dengan pengamanan autentikasi dokumen elektronik. Hasil tersebut ditandai dengan *cluster* yang digambarkan pada peta *mapping map*.
Dari temuan tersebut didapatkan banyak variasi cara penyandian sistem kriptografi untuk penyelamatan keamanan autentikasi dokumen elektronik. Peta menyiratkan bahwa jaringan antar tema-tema keduanya saling terkait. Semakin besar lingkaran pada gambar peta, maka semakin banyak variasi dari sistem penyandian kriptografi yang akan diteliti oleh peneliti, yaitu *access control, blockchain, cloud computing, cryptography, digital signature, encryption, and search encryption.* Selanjutnya semakin jauh dan kecil lingkarannya, maka terlihat antar tema-tema tersebut masih kurang mendapatkan perhatian maupun tema-tema lainnya yang masih jarang digunakan karena belum berkembang, seperti *anonymity, cloud storage, erc, hash function, provable, public key, smart contract,* dan sebagainya.

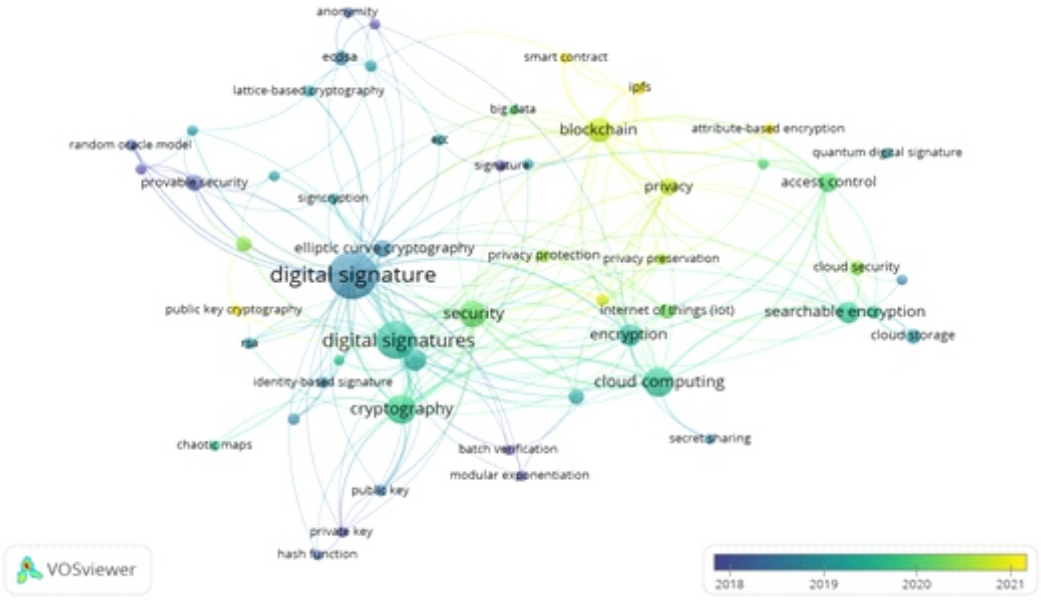
Hasil penelusuran pada pemetaan *network visualization* tentang sistem kriptografi pada pengamanan autentikasi dokumen elektronik yang ditemukan dari *mapping keyword* menghasilkan

Tabel 2
Grouping cluster, item and colour.

Cluster	***Item***	***Sum***	***Colour***
1	*Certificateless cryptography, code-based cryptography, digital signatures, elliptic curve, post-quantum cryptography, provable security, public key cryptography, random oracle model, rsa.*	9	*Red*
2	*Authentication, certificateless signature, elliptic curve cryptography, identity-based signature, pairing-free, security, and signcryption.*	7	*Light green*
3	*Batch verification, cloud computing, elliptic curve cryptography, encryption, modular exponentiation, secret sharing*	6	*Blue*
4	*Cloud security, cloud storage, data sharing, internet of things (iot), searchable encryption, searchable symmetric encryption.*	6	*Mustard*
5	*Chaotic maps, cryptography, digital signature, hash function, private key, public key.*	6	*Violet*
6	*Access control, attribute-based encryption, electronic medical records, internet of things (iot), privacy preservation, quantum digital signature.*	5	*Light Blue*
7	*Anonymity, bitcoin, ecdsa, lattice-based cryptography, ring signature.*	5	*Orange*
8	*Big data, blockchain, ipfs, privacy, smart contract.*	5	*Brown*
9	*Digital certificate, ecc, privacy protection, signature*	4	*Light Pink*

Sumber: *VOSViewer* 2022

b. .Overlay Visualization



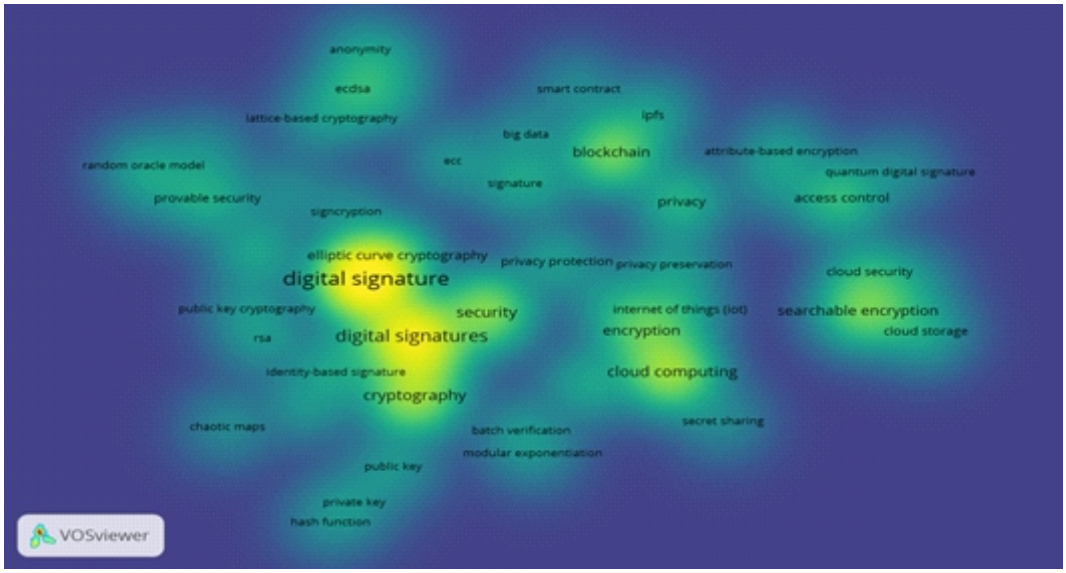
Gambar 2
Tampilan Peta *Overlay Visualization*
Sumber: *VOSViewer* 2022

sembilan *cluster* dengan berbagai warna yang berbeda, 54 *item* dengan rincian jumlah *keyword* seperti ditunjukkan pada Tabel 2.

Berdasarkan hasil peta *overlay visualization*, diketahui bahwa tahun 2020 adalah tahun paling banyak publikasi mengenai sistem kriptografi untuk pengamanan autentikasi dokumen elektronik. Hal ini ditandai dengan lingkaran berwarna hijau kebiruan (*spring green*) karena terdapat banyak jaringan tema-tema yang saling berhubungan antar tema lainnya menuju tema lingkaran berwarna hijau (*green*). Kemudian terlihat seberapa kuat dan lemahnya kekuatan jaringan antar tema-tema lainnya yang saling terhubung dalam peta *network* yang tercipta. Hasil yang diperoleh dari deskripsi tentang periode artikel penelitian antara tahun 2019 hingga tahun 2020, ditandai dengan berwarna biru menuju biru (*atlantic*) ditandai untuk menyatakan *keyword* pencarian tema-tema tersebar banyak digunakan untuk dipublikasikan pada penelitian. Tahun 2020 hingga tahun 2021, ditandai dengan warna hijau sampai kuning (*lime*) untuk menyatakan bahwa *keyword* tersebut masih belum banyak digunakan atau dipublikasikan untuk penelitiannya.

Number of publication research by year merupakan tentang publikasi mengenai

c. Density Visualization



Gambar 3
Tampilan peta *Density Visualization*
Sumber: *VOSViewer* 2022

sistem kriptografi untuk pengamanan autentikasi dokumen elektronik berdasarkan tahun publikasinya, yaitu a) tahun 2022 berjumlah 47 artikel jurnal; b) tahun 2021 berjumlah 24 artikel jurnal; c) tahun 2020 berjumlah 15 artikel jurnal; d) tahun 2019 berjumlah 19 artikel jurnal; d) tahun 2018 berjumlah 41 artikel jurnal; dan e) tahun 2017 berjumlah 31 artikel jurnal.

Berdasarkan hasil peta *density visualization*, terlihat warna hijau sedikit kekuningan (*lime*) yang berarti tema sistem kriptografi belum banyak variasi pembaruan yang dihasilkan dari penelitian sebelumnya ataupun tema-tema tersebut masih kurang disentuh atau dipublikasikan. Begitu juga sebaliknya warna kuning cerah (*light yellow*) yang berarti banyak dilakukan pembaruan dari hasil penelitian sebelumnya yang dapat dijadikan sebagai celah penelitian oleh peneliti selanjutnya dan bisa digunakan di masa yang akan datang.

Rq2: Berapa banyak penelitian yang relevan dengan sistem kriptografi pada pengamanan autentikasi dokumen elektronik?

Country-relevant search analysis by Scopus merupakan tentang publikasi mengenai sistem kriptografi untuk pengamanan autentikasi dokumen elektronik berdasarkan negara publikasinya dan jumlah publikasinya. Menunjukkan berbagai negara yang mempublikasikan bagaimana bentuk

Tabel 3
Relevant search analysis

Code	Title	Research	Journal	Year
R1	*Reduction of Cryptography processing upward in BGP security protocols: An investigation*	Dhir, S., Madhulika Agarwal, A,. Kapoor, A.	*International Mobile and Embedded technology Conference, pp.29-32*	2022
R2	*An Enhanced Cryptographic algorithm in securing healthcare medical records*	Paragas. J.R,.	*Proceeding - 2020 3rd International Conference on Vocational Education and Electrical Engineering : Strengthening the framework of Society 5.0*	2020
R3	*DBSR: A depth-based secure routing protocol; for underwater sensor networks*	Alharbi, A,.	*International Journal of Advanced Computer Science and Applications 11 (9), pp 628-634*	2020
R4	*Securing physical documents with digital signatures*	Winter, C., Berchtold, W., Hollenbeck. J.N	*IEEE 21st International Workshop on Multimedia Signal Processing, MMSP 2019*	2019
R5	*Analysis of attacks on mail disposition systems secured by digital signatures equipped with AES and RSA algorithms*	Siregar, H., Junaeti, E., Hayatno, T	*Pertanika Journal of science and Technology 26 (3), pp 1443-1452*	2018
R6	*Efficients weights threshold ECDSA for securing bitcoin wallet*	Dikshit, P. Singh. K	*ISEA Asia Security and Privacy Conference 2017, ISEASP 2017*	2017
R7	*An Efficient Elliptic Curve Cryptography Signature Server with GPU*	Pan, W., Zheng. F., Zhao, Y., Zhu, W.T., Jing, J	*IEEE Transaction on Information Forensics and Security 12(1), pp. 111-122*	2017

R8	*Benchmarking Cryptographic schemes for securing public cloud storages (practical experience report)*	Contiu, S., Leblond, E., Réveillère, L	*Lecture notes in computer (including subseries Lecture Notes in Artificial Intelligence and Lecture notes in Bioinformatics) pp. 163-176*	2017
R9	*Obfuscation and encryption for securing semiconductor supply chain*	Guin, U., tehranipoor., M.M	*Hardware protection through obfuscation pp. 317-345*	2017

Sumber: *Research Data* 2022

sistem kriptografi untuk pengamanan autentikasi dokumen elektronik di negaranya. Berikut antara lain: a) negara China berjumlah 35 artikel jurnal; b) negara India berjumlah 30 artikel jurnal; c) negara United States berjumlah 24 artikel jurnal; d) negara Germany berjumlah 14 artikel jurnal; e) negara Jepang berjumlah 12 artikel jurnal; f) negara Australia berjumlah 6 artikel jurnal; g) negara Saudi Arabia berjumlah 6 artikel jurnal; h) negara Kanada berjumlah 5 artikel jurnal; i) negara France berjumlah 5 artikel jurnal; dan j) negara Rusia berjumlah 5 artikel jurnal.

SIMPULAN

Hasil penelitian SLR menggunakan artikel jurnal dari Scopus dengan aplikasi *VOSviewer* menunjukkan terdapat sembilan *cluster* penelitian tentang sistem kriptografi pada pengamanan autentikasi dokumen elektronik. Artikel yang dijadikan rujukan dalam rentang waktu tahun 2017 hingga tahun 2020, publikasi terbanyak pada tahun 2020.

Berdasarkan hasil analisis terhadap sembilan artikel yang diseleksi ditemukan bahwa terdapat beberapa jenis sistem kriptografi yang digunakan untuk pengamanan kerahasiaan dan keaslian autentikasi dokumen elektronik di berbagai negara baru-baru ini yaitu *access control, blockchain, cloud computing, cryptography, digital signature, encryptiption, and searchable encryption.* Beberapa jenis penyandian sistem kriptografi yang masih jarang digunakan yaitu *anonymity, cloud storage, erc, hash function, provable, public key, smart contract,* dan sebagainya.

Berbagai negara yang sudah menerapkan sistem kriptografi pada pengamanan autentikasi dokumen elektronik berdasarkan tahun publikasi 2017-2022 adalah China, India, United States, Germany, Japan, Australia, Saudi Arabia, Canada, France, dan Russian. Pada *cluster keywords* menggunakan

VOSviewer untuk pemetaan didapatkan disimpulkan bahwa masih banyak peluang tema sistem kriptografi dikaji lebih dalam lagi. Selain *keywords*, penelitian yang akan datang juga dapat dikembangkan dari sisi metode penelitiannya.

DAFTAR PUSTAKA

Alharbi, A. (2020). DBSR: A Depth-Based Secure Routing Protocol for Underwater Sensor Networks. *Journal of Advanced Computer Science and Applications*, (pp. 9-11).https://pdfs.semanticscholar.org/8d57/ddcd883dcac98a5dbbbf6cb91d44e9ebf6ca.pdf

Chan, A.P.C., Javed, A. A,. Lyu, S., Hon, C. K. H., Wong, F. K. W. (2016). "Strategies for Improving Safety and Health of Ethnic Minority Construction workers." Journal of Construction Engineering and Management, Vol. 142(9). https://ascelibrary.org/doi/abs/10.1061/(ASCE)CO.1943-7862.0001148

Contiu, S., Leblond, E., & Réveillère, L. (2017, June). Benchmarking Cryptographic Schemes for Securing Public Cloud Storages. *In IFIP International Conference on Distributed Applications and Interoperable Systems* (pp. 163-176). Springer. https://link.springer.com/chapter/10.1007/978-3-319-59665-5_12

Dhir, S., Agarwal, A., & Kapoor, A. (2022, March). Reduction of Cryptography Processing Upward in BGP Security Protocols: An Investigation. *International Mobile and Embedded Technology Conference (MECON)* (pp. 29-32). IEEE. https://ieeexplore.ieee.org/abstract/document/9751875/?casa_token=Fhop452sgWIAAAAA:E2oNW_483um6hL4alwY1rasD5JVpU9u4K_tGhEv2T1P09J81kfs9T2LTU-KjtqTsDuMHyrODFSvN6wA

Dikshit, P., & Singh, K. (2017, January). *Efficient weighted threshold ECDSA for securing bitcoin wallet. ISEA Asia Security and Privacy (ISEASP)* (pp. 1-9). IEEE. https://ieeexplore.ieee.org/abstract/document/7976994/?casa_token=UB-c_IxfuFEAAAAA:X1oolxPExwIj1QckpDT5pKIbYNrmb_WkTA7AaBuOfh_kitPWU994IcOiuorHdnc5WJwuqZX8HjCaCWo

Guin, U., & Tehranipoor, M. M. (2017). Obfuscation and Encryption for Securing Semi Conductor Supply Chain. In *Hardware Protection through Obfuscation* (pp. 317-346). Springer. https://link.springer.com/chapter/10.1007/978-3-319-49019-9_13

Pan, W., Zheng, F., Zhao, Y., Zhu, W. T., & Jing, J. (2016). An Efficient Elliptic Curve Cryptography Signature Server with GPU Acceleration. *IEEE Transactions on Information Forensics and Security*, *12*(1), 111-122. https://ieeexplore.ieee.org/iel7/10206/4358835/07555336.pdf?casa_token=niIYr1mArIoAAAAA:B_wgIdX9O4kYjuq1PMoWz1-3j-Pzns3SMLzVkC_7rYrNxKj3PiTHnoHLKWL_EWOA4aRCLIRa45d-N84

Paragas, J. R. (2020, October). An Enhanced Cryptographic Algorithm in Securing Healthcare Medical Records. In *2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE)* (pp. 1-6). IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9243228&casa_token=AAxWFCxZ7_kAAAAA:dHhvh2s_QVVWv969riv2ZKysDZ6ZP_IIgnclz69jiCZfVKaO0WSj3rCREcyl3PbP0h8F2nSuIlVXlTc

Rosmasari., Dwi RA, R, A., Dengen, N., Taruk, M., 2018, Implementasi Metode Kriptografi International Data Encryption Algorithm (IDEA) Untuk Pengamanan Data Berita Publik Khatulistiwa Televisi Bontang, *Jurnal Teknologi Informasi*, (pp. 2-4). https://e-journals.unmul.ac.id/index.php/INF/article/view/1872/pdf

Siregar, H., Junaeti, E., & Hayatno, T. (2018). Analysis of Attacks on Mail Disposition Systems Secured by Digital Signatures Equipped with AES and RSA Algorithms. *Pertanika Journal of Science & Technology*, (pp. 26-29).http://www.pertanika.upm.edu.my/resources/files/Pertanika%20PAPERS/JST%20Vol.%2026%20(3)%20Jul.%202018/37%20JST(S)-0442-2018-3rdProof.pdf

Society of American Archivists. (2022). SAA dictionary: Authentication. SAA.https://dictionary.archivists.org/entry/authentication.html

Winter, C., Berchtold, W., & Hollenbeck, J. N. (2019, September). Securing Physical Documents with Digital Signatures. In *2019 IEEE 21st International Workshop on Multimedia Signal Processing (MMSP)* (pp. 1-6).IEEE.https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8901807