Terbit online pada laman web jurnal: **http://journal.isas.or.id/index.php/JACOST**

JOURNAL OF APPLIED COMPUTER SCIENCE AND TECHNOLOGY (JACOST)

Vol. 7 No. 1 (2026) 22 – 31 | ISSN: 2723-1453 (Media Online)

Paradoks Keamanan Autentikasi Dua Faktor (2FA): *Systematic Literature Review* terhadap Kesenjangan Protokol Teoretis dan Kegagalan Implementasi Praktis

Dzikri Izzatul Haq[1], Syafrial Fachri Pane[2]
[1,2]Sekolah Vokasi, Sarjana Terapan Teknik Informatika, Universitas Logistik dan Bisnis Internasional
[1]1214062@std.ulbi.ac.id, [2]syafrial.fachri@ulbi.ac.id

Abstract

Two-Factor Authentication (2FA) has been widely adopted as a fundamental security standard, yet sophisticated cyberattacks continue to exploit security loopholes that often lie not in the protocol itself, but in its implementation. This study aims to systematically synthesize current scientific literature to uncover the root causes of the gap between the theoretical security of 2FA protocols and practical exploitation risks in the field. Using the Systematic Literature Review (SLR) method with PRISMA guidelines, 43 high-quality articles (Q1-Q4) from the Scopus database published between 2020 and 2025 were analyzed using thematic synthesis. The findings reveal a central paradox where, although 2FA protocols are becoming mathematically stronger, 88% of failure points have shifted to implementation fundamentals; the most critical weaknesses identified are the storage of secret keys in plaintext format on client applications and the effectiveness of social engineering attacks against users. This study concludes that real-world 2FA security is determined more by the quality of implementation code and user awareness than by the cryptographic strength of the protocol alone, implying that industry priorities must shift from developing new protocols to enforcing secure implementation audits and continuous user education.

Keywords: application security, cybersecurity, exploitation, systematic literature review, two-factor authentication

Abstrak

Autentikasi Dua Faktor (2FA) telah diadopsi secara luas sebagai standar keamanan fundamental, namun serangan siber canggih terus mengeksploitasi celah keamanan yang sering kali bukan terletak pada protokolnya, melainkan pada implementasinya. Penelitian ini bertujuan untuk mensintesis literatur ilmiah terkini guna mengungkap akar penyebab kesenjangan antara keamanan teoretis protokol 2FA dan risiko eksploitasi praktis di lapangan. Menggunakan metode *Systematic Literature Review* (SLR) dengan pedoman PRISMA, sebanyak 43 artikel berkualitas tinggi (Q1-Q4) dari basis data Scopus yang diterbitkan antara tahun 2020-2025 dianalisis menggunakan sintesis tematik. Hasil temuan menunjukkan sebuah paradoks utama bahwa meskipun protokol 2FA semakin kuat secara matematis, 88% titik kegagalan bergeser ke fundamental implementasi, dengan kelemahan paling kritis berupa penyimpanan *secret key* dalam format *plaintext* pada aplikasi klien serta efektivitas serangan rekayasa sosial terhadap pengguna. Studi ini menyimpulkan bahwa keamanan 2FA di dunia nyata lebih ditentukan oleh kualitas kode implementasi dan kesadaran pengguna daripada kekuatan kriptografi protokol semata, sehingga prioritas industri harus digeser dari pengembangan protokol baru ke arah penegakan audit implementasi yang aman dan edukasi pengguna yang berkelanjutan.

Kata kunci: autentikasi dua faktor, eksploitasi, keamanan aplikasi, keamanan siber, tinjauan literatur sistematis

1. Pendahuluan

Di era digital saat ini, persaingan untuk menyediakan layanan yang aman dan terpercaya menjadi krusial. Autentikasi pengguna, sebagai gerbang utama akses ke sistem digital, memegang peranan vital. Metode autentikasi tradisional yang hanya mengandalkan kata sandi (faktor tunggal) semakin terbukti tidak memadai dalam menghadapi lanskap ancaman siber yang terus berkembang, seperti serangan phishing, brute-force, dan kebocoran data [1], [2].

Sebagai solusi, Autentikasi Dua Faktor (2FA) telah diadopsi secara luas sebagai standar industri untuk meningkatkan keamanan akun. 2FA menambahkan lapisan verifikasi kedua, yang mengharuskan pengguna untuk membuktikan identitas mereka tidak hanya dengan "sesuatu yang mereka tahu" (kata sandi), tetapi juga dengan "sesuatu yang mereka miliki" (seperti ponsel yang menerima kode OTP) atau "sesuatu yang melekat pada diri mereka" (seperti sidik jari) [3], [4].

Evolusi metode autentikasi telah menjadi subjek penelitian yang intensif dalam satu dekade terakhir.

Secara tradisional, penelitian keamanan berfokus pada transisi dari *Single Factor Authentication* (SFA) menuju 2FA untuk menanggulangi kelemahan kata sandi statis. Studi-studi awal, seperti yang dilakukan oleh Yin et al. [5], mengevaluasi kerentanan skema OTP berbasis SMS dan mengusulkan alternatif berbasis pohon Merkle (MOTP) untuk menghindari penyimpanan kunci di sisi server. Literatur kemudian berkembang ke arah autentikasi biometrik dan perilaku (*behavioral biometrics*), di mana Bian et al. [6] dan Wang et al. [7] mengeksplorasi penggunaan sidik jari dan pola perilaku pengguna sebagai faktor kedua yang lebih sulit dipalsukan dibandingkan token fisik atau digital.

Meskipun adopsi 2FA telah terbukti efektif dalam mengurangi risiko pembobolan akun, lanskap riset modern menunjukkan adanya masalah keamanan yang persisten dan berlapis karena ancaman terus berevolusi. Penyerang mengembangkan teknik-teknik baru untuk melewati perlindungan 2FA, seperti serangan rekayasa sosial yang canggih untuk mencuri kode OTP atau serangan Man-in-the-Middle (MITM) untuk membajak sesi autentikasi. Titik lemah seringkali tidak hanya terletak pada desain teoretis protokol, tetapi juga pada berbagai lapisan praktisnya. Studi forensik oleh Berrios et al. [8] secara gamblang membuktikan adanya kegagalan di level implementasi, di mana aplikasi 2FA populer sekalipun ditemukan menyimpan secret key dalam format plaintext, yang secara efektif meniadakan lapisan keamanannya.

Kerentanan ini diperparah dengan kelemahan di level protokol standar, seperti yang ditunjukkan oleh Hu et al. [9] yang berhasil menemukan celah serangan pelacakan lokasi pada protokol autentikasi 5G. Di lapisan terluar, terdapat ancaman pada konteks pengguna, di mana model ancaman untuk layanan krusial seperti mobile money menunjukkan bahwa rekayasa sosial dan phishing tetap menjadi metode yang efektif untuk membajak kode OTP dan melewati perlindungan 2FA [10]. Selain itu, setiap metode 2FA memiliki kelebihan dan kekurangannya sendiri dalam hal keamanan, usability, dan biaya. Metode populer seperti OTP SMS terbukti rentan terhadap serangan SIM swapping [5], sementara metode biometrik menghadapi tantangan privasi dan kemungkinan pemalsuan [6].

Meskipun berbagai studi telah membahas keamanan 2FA, literatur yang ada saat ini cenderung terfragmentasi. Kesenjangan literatur (*research gap*) yang signifikan terlihat jelas pada kurangnya sintesis yang menghubungkan antara desain protokol kriptografi dengan praktik implementasi di sisi klien (*client-side implementation*). Studi forensik terbaru oleh Berrios et al. [8] dan analisis kerentanan OAuth 2.0 oleh Munonye & Péter [4] mulai mengungkap bahwa aplikasi populer sering kali gagal menerapkan standar enkripsi penyimpanan data yang memadai. Adapun studi-studi tersebut memiliki cakupan yang sangat spesifik, sementara studi lainnya fokus pada aspek *usability* pengguna. Sebagai contoh, Ali et al. [11] melakukan tinjauan mendalam terhadap model ancaman pada *mobile money*, namun membatasi konteksnya hanya pada transaksi keuangan tanpa menyentuh aplikasi umum. Di sisi lain, Hu et al. [10] dan Fei & Wang [12] memfokuskan analisis mereka pada lapisan protokol jaringan, khususnya kerentanan *Authentication and Key Agreement* (AKA) pada jaringan 5G dan LTE. Sementara itu, tinjauan aspek manusia yang dilakukan oleh Marky et al. [13] sangat komprehensif dalam membahas persepsi dan kelelahan pengguna (*security fatigue*), namun kurang membahas aspek teknis implementasi perangkat lunak. Adapun kurangnya tinjauan sistematis yang secara spesifik memetakan bagaimana kegagalan implementasi teknis (seperti manajemen kunci yang buruk) dapat meruntuhkan protokol yang secara teoretis aman. Belum ada tinjauan sistematis yang secara khusus mengagregasi bukti-bukti empiris kegagalan implementasi ini untuk dikontraskan dengan kekuatan teoretis protokolnya.

Oleh karena itu, tinjauan literatur sistematis ini bertujuan untuk mengisi celah tersebut untuk memetakan secara holistik "paradoks keamanan" tersebut, melengkapi studi-studi terdahulu yang lebih berfokus pada desain protokol atau studi pengguna secara terpisah, dengan mengidentifikasi, mengevaluasi, dan mensintesis penelitian yang diterbitkan antara tahun 2020 hingga 2025. Kebaruan (*novelty*) dari studi ini terletak pada fokus analisisnya yang tidak hanya membandingkan "metode apa yang terbaik", tetapi menjawab "mengapa metode terbaik tetap gagal" dengan menyoroti vektor serangan pada lapisan implementasi praktis. Kontribusi utama artikel ini adalah menyediakan landasan bagi praktisi untuk memahami bahwa risiko terbesar saat ini bukan lagi pada pemecahan sandi, melainkan pada celah integrasi sistem, serta memberikan kontribusi berupa sintesis berbasis bukti yang menjadi landasan bagi praktisi dalam memitigasi risiko implementasi sistem autentikasi.

2. Metode Penelitian

Penelitian ini menggunakan metode *Systematic Literature Review* (SLR) yang mengikuti protokol PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). SLR adalah metode tinjauan literatur yang mengidentifikasi, mengevaluasi, dan menginterpretasikan semua hasil dari suatu topik penelitian untuk menjawab pertanyaan penelitian tertentu secara sistematis [14], [15]. Metode ini diterapkan secara sistematis sesuai langkah dan protokol yang membantu menghindari pemahaman subjektif dan bias dalam proses kajian literatur. Kerangka kerja PRISMA dipilih dan digunakan dalam penelitian ini untuk menjamin transparansi, validitas, dan reproduktifitas proses seleksi studi. Penggunaan diagram alir PRISMA berfungsi strategis untuk memetakan proses eliminasi artikel dari 340 data mentah

DOI : https://doi.org/10.52158/h9qv3j56

menjadi 43 data final, sehingga meminimalkan bias seleksi subjektif peneliti dan memastikan bahwa literatur yang dianalisis relevan secara objektif terhadap pertanyaan penelitian.

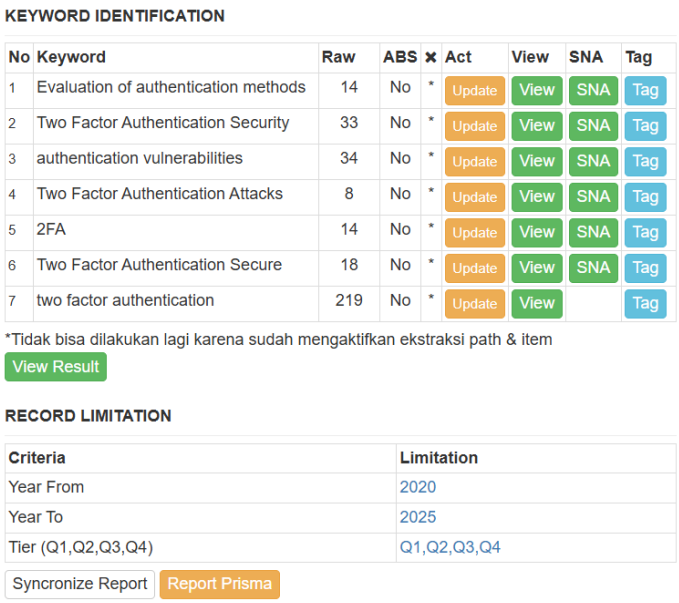
2.1. Pertanyaan Penelitian (*Research Questions*)

Untuk mencapai tujuan penelitian secara sistematis, studi ini dipandu oleh tiga pertanyaan penelitian utama. Pertanyaan pertama (RQ1) bertujuan mengevaluasi efektivitas mekanisme keamanan yang diterapkan pada aplikasi 2FA dalam mencegah eksploitasi praktis. Pertanyaan kedua (RQ2) difokuskan untuk mengidentifikasi jenis-jenis serangan yang paling dominan dilaporkan dalam literatur terbaru. Pertanyaan ketiga (RQ3) disusun untuk menganalisis perbedaan tingkat keamanan antar jenis 2FA guna membangun hierarki pertahanan ditinjau dari sudut pandang implementasi dan vektor serangan.

Tahapan SLR yang dilakukan mengikuti metodologi PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), yang meliputi identifikasi, penyaringan, kelayakan, dan inklusi.

2.2. Sumber Data dan Strategi Pencarian

Tahapan yang pertama yaitu penentuan database dan kata kunci. Pencarian literatur dilakukan melalui basis data akademik Scopus yang dipilih karena reputasinya dalam mengindeks jurnal teknik informatika berkualitas tinggi. Untuk mengoptimalkan akurasi pencarian dan pengelolaan metadata, penulis menggunakan bantuan perangkat lunak Watase (sebagai *tools* manajemen referensi dan *harvesting* metadata). Kata kunci yang digunakan adalah: *"Evaluation of Authentication Methods"*, *"Two Factor Authentication Security"*, *"Authentication Vulnerabilities"*, *"Two Factor Authentication Attacks"*, *"2FA"*, *"Two Factor Authentication Secure"*, dan *"Two Factor Authentication"*. Hasil identifikasi awal berdasarkan kata kunci dapat dilihat pada Gambar 1.



KEYWORD IDENTIFICATION

No	Keyword	Raw	ABS	✖	Act	View	SNA	Tag
1	Evaluation of authentication methods	14	No	*	Update	View	SNA	Tag
2	Two Factor Authentication Security	33	No	*	Update	View	SNA	Tag
3	authentication vulnerabilities	34	No	*	Update	View	SNA	Tag
4	Two Factor Authentication Attacks	8	No	*	Update	View	SNA	Tag
5	2FA	14	No	*	Update	View	SNA	Tag
6	Two Factor Authentication Secure	18	No	*	Update	View	SNA	Tag
7	two factor authentication	219	No	*	Update	View		Tag

*Tidak bisa dilakukan lagi karena sudah mengaktifkan ekstraksi path & item

View Result

RECORD LIMITATION

Criteria	Limitation
Year From	2020
Year To	2025
Tier (Q1,Q2,Q3,Q4)	Q1,Q2,Q3,Q4

Syncronize Report | Report Prisma

Gambar 1. Hasil Identifikasi Kata Kunci dari Watase

2.3. Kriteria Inklusi dan Eksklusi

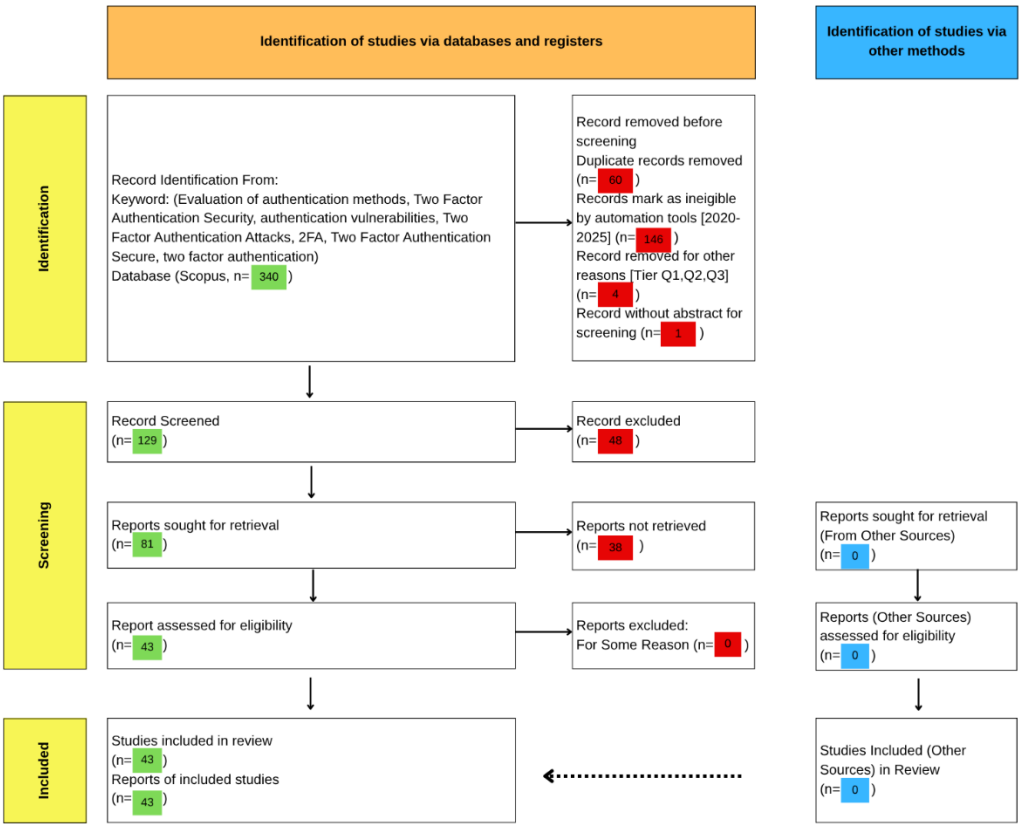
Kemudian untuk tahapan kedua adalah penentuan kriteria inklusi dan eksklusi. Berdasarkan topik evaluasi keamanan 2FA yang akan dibahas, kriteria inklusi yang ditetapkan dalam penelitian ini mencakup artikel yang diterbitkan antara 1 Januari 2020 hingga 31 Desember 2025, merupakan naskah lengkap (*full paper*) yang terindeks Scopus (Tier Q1, Q2, Q3, Q4), dan memiliki topik utama yang membahas evaluasi keamanan atau mekanisme 2FA.

Sebaliknya, kriteria eksklusi diterapkan secara ketat pada artikel yang berada di luar rentang waktu tersebut, bukan merupakan naskah lengkap (*full paper*), memiliki topik yang tidak relevan, merupakan duplikasi, atau tidak memiliki abstrak.

2.4. Seleksi Studi dan Ekstraksi Data

Selanjutnya ada proses seleksi. Proses seleksi studi didokumentasikan dalam diagram alir PRISMA (Gambar 2). Dari 340 artikel yang teridentifikasi, setelah melalui tahap penyaringan (penghapusan duplikat, skrining judul dan abstrak, serta asesmen kelayakan teks penuh), diperoleh 43 studi yang memenuhi kriteria untuk dianalisis secara mendalam.

DOI : https://doi.org/10.52158/h9qv3j56



Gambar 2. Diagram Alir PRISMA untuk Seleksi Studi

2.5. Ekstraksi Data dan Sintesis Temuan

Setelah 43 studi final terpilih, proses ekstraksi data dianalisis menggunakan teknik Sintesis Tematik yang mencakup tiga tahapan utama. Tahap pertama adalah *coding*, yaitu pelabelan temuan spesifik seperti penyimpanan *plaintext* atau serangan MITM. Tahap kedua adalah *grouping*, di mana label-label tersebut dikelompokkan ke dalam tema besar meliputi Protokol, Implementasi, dan Manusia. Tahap ketiga adalah *interpretation*, yaitu melakukan sintesis naratif untuk menjawab pertanyaan penelitian (RQ). Dari setiap artikel, diekstraksi informasi kunci yang mencakup: mekanisme atau protokol 2FA yang dibahas, jenis kerentanan atau vektor serangan yang diidentifikasi, metode keamanan yang diusulkan atau dievaluasi, serta konteks penelitian (misalnya IoT, cloud, 5G).

Data kualitatif yang terkumpul kemudian disintesis menggunakan pendekatan analisis tematik. Temuan-temuan dari setiap artikel dikelompokkan ke dalam tema-tema utama yang selaras dengan pertanyaan penelitian. Untuk RQ1 (efektivitas), tema difokuskan pada faktor-faktor keberhasilan dan kegagalan implementasi. Untuk RQ2 (jenis serangan), serangan diklasifikasikan berdasarkan targetnya. Terakhir, untuk RQ3 (tingkat keamanan), data dari berbagai artikel diintegrasikan untuk membangun hierarki keamanan berdasarkan bukti-bukti ancaman praktis yang dilaporkan.

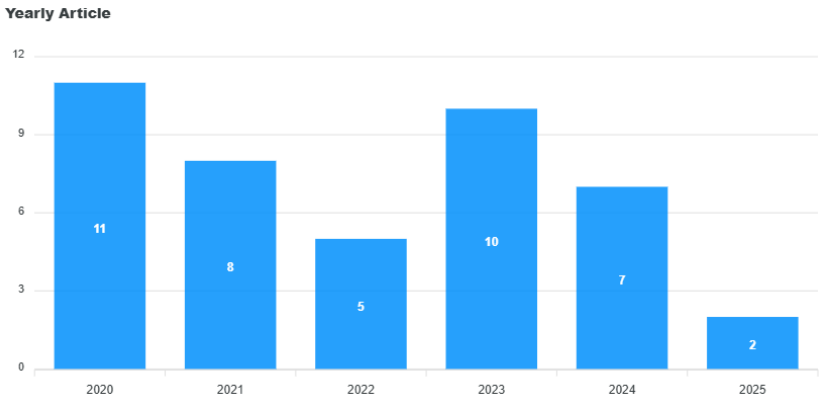
3. Hasil dan Pembahasan

Pada awal pencarian, peneliti menggunakan kriteria untuk dimasukkan ke dalam basis data, yaitu artikel dan jurnal yang mempelajari hubungan antara evaluasi keamanan dan mekanisme 2FA. Kemudian menerapkan kriteria inklusi dan eksklusi dengan melihat periode publikasi dari 2020 hingga 2025. Proses penyaringan dan persyaratan kelayakan menghasilkan 43 jurnal penelitian yang relevan.

Dari 43 artikel yang terpilih, dilakukan ekstraksi data untuk mendapatkan gambaran umum mengenai tren penelitian. Gambar 3 menunjukkan distribusi artikel berdasarkan tahun publikasi, di mana terlihat adanya minat penelitian yang konsisten pada topik ini dari tahun 2020 hingga 2025, dengan puncak signifikan pada tahun 2020 dan 2023. Lonjakan di tahun 2020 kemungkinan besar dipicu oleh pandemi COVID-19, yang mengakselerasi transformasi digital dan kerja jarak jauh secara masif, sehingga meningkatkan urgensi penelitian mengenai keamanan autentikasi. Minat yang kembali tinggi pada tahun 2023 menunjukkan bahwa topik ini tetap sangat relevan seiring dengan munculnya vektor

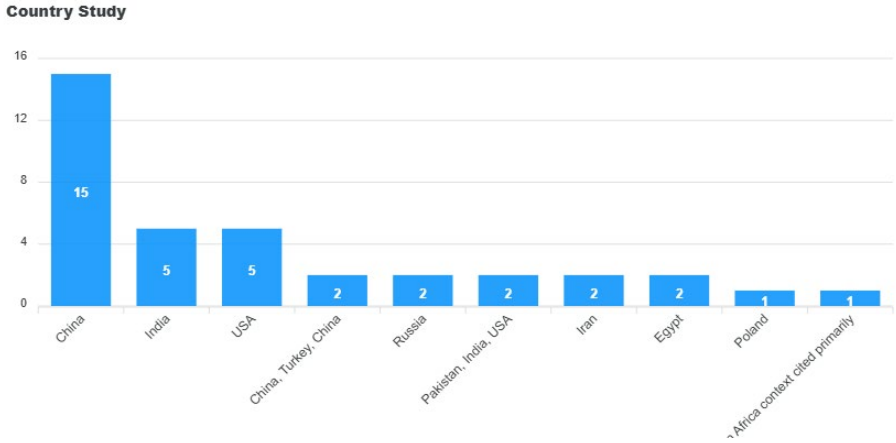
DOI : https://doi.org/10.52158/h9qv3j56

serangan yang lebih canggih untuk menembus 2FA di era pasca-pandemi.



Gambar 3. Jumlah Artikel Berdasarkan Tahun Publikasi

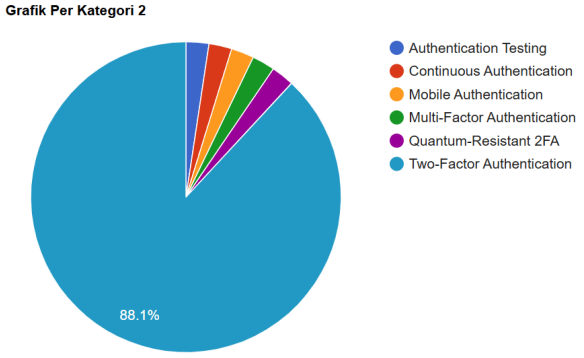
Distribusi geografis dari studi yang direview menunjukkan bahwa penelitian mengenai 2FA dilakukan secara global, dengan konsentrasi tertinggi di China, India, dan Amerika Serikat, seperti yang ditunjukkan pada Gambar 4. Dominasi ini bukanlah kebetulan, melainkan cerminan status ketiga negara tersebut sebagai pemimpin ekonomi digital global. Dengan jumlah pengguna internet terbesar dan menjadi rumah bagi industri teknologi raksasa, negara-negara ini memiliki kebutuhan keamanan siber yang sangat tinggi. Skala yang masif ini menjadikan mereka pusat inovasi sekaligus target utama serangan siber, sehingga secara alami mendorong produktivitas riset yang sangat tinggi di bidang keamanan autentikasi untuk melindungi ekosistem digital mereka.



Gambar 4. Distribusi Artikel Berdasarkan Negara Studi Kasus

Terakhir, Gambar 5 menyajikan distribusi artikel berdasarkan kategori utamanya. Data ini menunjukkan bahwa mayoritas absolut, yaitu 88.1%, dari studi yang dianalisis secara spesifik berfokus pada "Two-Factor Authentication". Angka yang sangat tinggi ini berfungsi sebagai validasi metodologis. Hal ini mengonfirmasi bahwa strategi pencarian kata kunci dan kriteria seleksi yang diterapkan telah berhasil mengumpulkan kumpulan data yang sangat fokus dan relevan dengan topik penelitian, sehingga memperkuat validitas dari kesimpulan yang akan ditarik dalam studi ini.

Tabel 1 menyajikan pemetaan komprehensif dari 43 studi terpilih yang menjadi landasan utama analisis ini, mencakup penulis, tahun, metode/model yang diusulkan, dan konteks penelitiannya. Data dalam tabel ini merinci metode yang dievaluasi dan konteks penggunaannya, yang selanjutnya akan diuraikan secara mendalam di bagian Pembahasan untuk menjawab pertanyaan penelitian terkait efektivitas dan kerentanan 2FA.



Gambar 5. Distribusi Artikel Berdasarkan Kategori Utama

DOI : https://doi.org/10.52158/h9qv3j56

Bagian selanjutnya membahas temuan-temuan kunci dari 43 studi yang dianalisis untuk menjawab pertanyaan penelitian. Pembahasan difokuskan pada interpretasi hasil, implikasi, dan perbandingan dengan literatur yang ada untuk menyoroti kontribusi penelitian.

Tabel 1. Jurnal Target

No	Authors	Year	Method	Context
1	[1]	2020	Provably Secure 2FA Scheme for USB	Proposes an ECC-based protocol for USB storage devices
2	[2]	2022	2FA Framework for Cloud Computing	Uses OTP and nonces to secure cloud access
3	[3]	2020	2FA Protocol for 5G Networks	Uses self-certified public key cryptography for multi-server environments
4	[4]	2022	OAuth 2.0 Vulnerability Detection	Uses Machine Learning to detect vulnerabilities in the OAuth flow
5	[5]	2020	MOTP (Merkle Tree-based OTP)	OTP scheme that does not require storing a secret key on the server
6	[6]	2020	Bio-AKA (Biometrics + PUF)	Combines fingerprint and PUF for user and device authentication
7	[7]	2021	Quantum2FA	A quantum-resistant 2FA scheme based on smart cards and lattice cryptography
8	[8]	2023	Forensic Analysis of 2FA Apps	Discovers insecure secret key storage in popular applications
9	[9]	2022	Provably Secure 2FA Protocol for IoT	Analyzes and fixes weaknesses in authentication protocols for WSNs
10	[10]	2020	Vulnerability in 5G Authentication Protocols	Discovers a location tracking attack on the 5G AKA protocol
11	[11]	2020	Review of 2FA Threat Models for Mobile Money	Analyzes threat models and countermeasures for mobile money 2FA
12	[12]	2023	Vulnerability of AKA Protocol in LTE/5G	Analyzes vulnerabilities and enhancements of mobile authentication protocols
13	[13]	2022	User Perceptions of 2FA	Analyzes user perceptions and usability issues of various 2FA methods
14	[14]	2021	Systematic Framework for 2FA Analysis	Proposes a framework to analyze smart card-based 2FA schemes
15	[15]	2022	Low-Area 2FA Design for IoT	Uses DIES and SBI for IoT security with minimal hardware usage
16	[16]	2023	ECC-based 2FA Protocol	A robust and effective 2FA protocol for mobile computing
17	[17]	2019	Influence of Incentives on 2FA Adoption	Analyzes whether incentives (e.g., game items) increase 2FA adoption
18	[18]	2021	2FA Scheme with Graphical Password	Design and implementation of 2FA that does not require a verifier table
19	[19]	2020	Securing 2FA Communication	Uses post-quantum cryptosystem to secure SMS OTP
20	[20]	2020	VoIP Voicemail Security System	Uses 2FA and biometrics to secure voicemail
21	[21]	2023	2FA Scheme for Moodle E-Learning Platform	Proposes 2FA with digital certificates to enhance Moodle's security
22	[22]	2023	2FA with Biometric Voice Verification	Enhancing web application security with voice verification
23	[23]	2025	Metamorphic Testing for Auth Vulnerabilities	Uses GUI-based testing to detect vulnerabilities in Android apps
24	[24]	2020	Lightweight 2FA Scheme for WBAN	Proposes a hash-chain based scheme for healthcare IoT
25	[25]	2021	Attacks and Solutions for a 2FA Protocol for WBAN	Analyzes and fixes weaknesses in authentication protocols for WBAN
26	[26]	2021	Blockchain-based 2FA Scheme	Uses blockchain and fuzzy extractor for identity authentication
27	[27]	2025	2FA for Intellectual Property Transactions	Uses zero-knowledge proof and biometrics for secure transactions
28	[28]	2024	2FAKA-C/S (2FA for Federated Learning)	Authentication and key agreement protocol for data transmission in Federated Learning
29	[29]	2021	2FA with Supervisor Authorization	Authentication for critical infrastructure requiring supervisor approval
30	[30]	2023	2FA Framework for Social IoMT	Uses Federated Learning for lightweight authentication in IoMT
31	[31]	2023	Provably Secure ECC-Based 2FA Scheme	A remote authentication protocol with session key agreement
32	[32]	2023	2L-MFA (2FA for IoT with Blockchain)	Uses blockchain and multi-factors for IoT device and user authentication
33	[33]	2021	ICAS (Identity-Concealed 2FA)	An identity-concealing 2FA scheme for remote servers
34	[34]	2020	2FA Offloading for Mobile Cloud	Proposes offloading authentication applications to the cloud for security
35	[35]	2022	PiGy (Piezo-Gyro Channel 2FA)	Transmits OTP from a token to a phone via acoustic vibrations

DOI : https://doi.org/10.52158/h9qv3j56

Tabel 1. (Lanjutan)

No	Authors	Year	Method	Context
36	[36]	2024	Wi-Fi-Based Environmental 2FA	Leverages Machine Learning for continuous two-factor authentication
37	[37]	2021	MagAuth (Behavioral Biometrics)	Secure and Usable Two-Factor Authentication with Magnetic Wrist Wearables
38	[38]	2020	BlinKey (2FA for VR)	Uses eye blink rhythm and pupil variation as 2FA in VR devices
39	[39]	2022	Haptic2FA	Haptics-Based Accessible Two-Factor Authentication for Blind and Low Vision People
40	[40]	2023	ZITA (Zero-Interaction 2FA)	Authentication without user interaction using contact traces and RF proximity
41	[41]	2024	PUPGUARD (Behavioral Biometrics)	Analyzes finger press patterns to defeat puppet attacks
42	[42]	2024	Cue-2FA	Separates visual cues and response input to counter shoulder surfing
43	[43]	2023	2FA for Digital Signatures	Uses a security token with biometric data (fingerprint)

3.1. Efektivitas Mekanisme Keamanan 2FA (RQ1)

Efektivitas sebuah mekanisme 2FA sangat bergantung pada desain protokol, kualitas implementasi, dan konteks penggunaannya. Literatur menunjukkan bahwa metode berbasis kriptografi asimetris (seperti ECC) dan perangkat keras khusus (seperti PUF) menawarkan keamanan teoretis tertinggi [16], [13]. Namun, faktor paling kritis yang menentukan efektivitas di dunia nyata adalah kualitas implementasi. Studi forensik oleh [8] secara gamblang menunjukkan bahwa aplikasi 2FA populer pun bisa menjadi sangat tidak aman jika kunci rahasia disimpan sebagai teks biasa di perangkat klien.

Hal ini diperkuat oleh studi kasus praktis yang mendemonstrasikan bahwa aplikasi seperti Aegis Authenticator dan TOTP Authenticator menyimpan *secret key* dalam format JSON dan XML tanpa enkripsi, sehingga sangat rentan terhadap eksploitasi. Sebaliknya, aplikasi seperti 2FAS dan Okta Verify menunjukkan praktik yang lebih aman dengan menerapkan enkripsi basis data yang dilindungi kata sandi [44]. Selain itu, efektivitas juga dipengaruhi oleh adopsi pengguna, di mana insentif terbukti dapat meningkatkan tingkat adopsi [17].

3.2. Jenis-jenis Serangan Paling Umum (RQ2)

Serangan terhadap 2FA dapat diklasifikasikan berdasarkan target utamanya. Yang pertama adalah serangan rekayasa sosial, khususnya *Phishing,* yang tetap menjadi ancaman paling dominan, terutama untuk metode berbasis OTP, di mana pengguna ditipu untuk menyerahkan kode mereka [11]. Yang kedua yaitu serangan pada protokol dan jaringan, seperti serangan *Man-in-the-Middle* (MITM) [16] dan serangan pelacakan lokasi (*linkability attack*) pada jaringan 5G [10] menunjukkan bahwa bahkan protokol standar pun bisa memiliki celah. Yang ketiga adalah serangan pada perangkat klien. Serangan ini adalah vektor serangan yang paling merusak.

Ekstraksi kunci rahasia dari perangkat yang terinfeksi malware [8] dan sensor capture attack pada perangkat IoT [9] dapat sepenuhnya meniadakan keamanan 2FA. Sebuah demonstrasi eksploitasi menunjukkan bahwa setelah *secret key* berhasil diekstraksi dari penyimpanan *plaintext* aplikasi, kode OTP yang identik dapat direplikasi menggunakan *library* seperti PyOTP, yang secara efektif memungkinkan pembajakan autentikasi (*authentication bypass*) [44]. Dan yang terakhir yaitu serangan pada server seperti Stolen-verifier attack, di mana penyerang mencuri *database* verifier, menjadi ancaman serius. Metode seperti MOTP [5] dan skema tanpa tabel verifier [18] dirancang khusus untuk menahan serangan ini.

3.3. Perbedaan Tingkat Keamanan Antar Jenis 2FA (RQ3)

Berdasarkan sintesis data, terbentuk hierarki keamanan yang jelas di antara berbagai metode 2FA. Tingkat terendah ditempati oleh Implementasi 2FA yang lemah dengan penyimpanan kunci tidak aman, diikuti oleh tingkat rendah yang mencakup 2FA berbasis SMS dan email karena kerentanannya terhadap SIM swapping dan phishing. Kemudian, tingkat menengah diisi oleh OTP berbasis aplikasi (TOTP) dan notifikasi push standar. Tingkat tinggi mencakup metode yang menggunakan biometrik canggih (terutama perilaku), kanal tersembunyi, dan skema OTP yang tidak bergantung pada rahasia bersama di server (seperti MOTP). Tingkat sangat tinggi dipegang oleh protokol yang terbukti aman secara formal, menggunakan kriptografi asimetris yang kuat (ECC), dan dirancang khusus untuk menahan serangan tingkat lanjut seperti insider attack. Dan yang terakhir yaitu tingkat tertinggi atau masa depan adalah metode yang tahan terhadap serangan komputasi kuantum [7], [19].

Kerangka kerja evaluasi sistematis [14] mengonfirmasi bahwa banyak skema yang diusulkan gagal memenuhi beberapa kriteria keamanan dasar, yang semakin mempertegas adanya tingkatan keamanan ini.

3.4. Komparasi dengan Studi Terdahulu

Temuan penelitian ini memperluas perspektif yang sebelumnya diajukan oleh Ali et al. [11] yang membatasi analisis ancaman pada konteks *mobile money*. Studi

DOI : https://doi.org/10.52158/h9qv3j56

kami menemukan bahwa kerentanan implementasi, khususnya penyimpanan kunci tidak aman seperti yang ditemukan oleh Berrios et al. [8], merupakan masalah sistemik di berbagai jenis aplikasi, bukan hanya finansial.

Hal ini menegaskan bahwa *gap* keamanan terbesar saat ini bukan lagi pada desain kriptografi protokol (seperti yang banyak dibahas pada studi 2020), melainkan pada kedisiplinan pengembang aplikasi dalam menerapkan standar keamanan (*secure coding*). Temuan ini menggeser diskursus dari "mana protokol terkuat" menjadi "bagaimana mengamankan implementasi".

3.5. Implikasi, Keterbatasan, dan Kontribusi Ilmiah

Temuan dari tinjauan ini memiliki implikasi penting. Bagi praktisi dan pengembang perangkat lunak, temuan bahwa kegagalan implementasi, khususnya penyimpanan secret key yang tidak aman merupakan akar masalah utama yang menjadi sebuah peringatan keras. Ini mengimplikasikan bahwa prioritas pengembangan harus bergeser dari sekadar mengadopsi protokol 2FA ke arah penerapan praktik coding yang aman, seperti pemanfaatan API penyimpanan kredensial sistem operasi (misalnya, Android Keystore atau iOS Keychain). Sedangkan bagi organisasi, dominasi serangan rekayasa sosial menegaskan bahwa solusi teknis saja tidak cukup. Diperlukan investasi berkelanjutan dalam program edukasi dan pelatihan kesadaran keamanan bagi pengguna untuk membangun pertahanan yang holistik.

Namun, penelitian ini memiliki beberapa keterbatasan yang perlu diakui. Pertama, pencarian literatur hanya terbatas pada basis data Scopus. Ada kemungkinan terdapat artikel relevan dari basis data lain seperti IEEE Xplore atau ACM Digital Library yang tidak teridentifikasi. Kedua, sebagai sebuah tinjauan literatur sistematis, studi ini bergantung pada data dan temuan yang dilaporkan oleh penelitian primer. Validitas kesimpulan kami secara inheren terikat pada kualitas dan akurasi dari 43 studi yang dianalisis. Terakhir, pemilihan kata kunci pencarian dapat menimbulkan bias yang memengaruhi hasil seleksi studi.

Meskipun demikian, kontribusi utama dari penelitian ini adalah menyediakan sintesis berbasis bukti yang menggeser fokus diskursus keamanan 2FA. Alih-alih hanya membandingkan kekuatan teoretis antar protokol, tinjauan ini secara tegas menyoroti kesenjangan antara keamanan teoretis dan risiko praktis. Dengan memetakan kegagalan implementasi dan serangan pada perangkat klien sebagai vektor ancaman paling kritis, penelitian ini memberikan landasan empiris bagi komunitas riset dan praktisi untuk lebih memprioritaskan keamanan di level implementasi—sebuah area yang seringkali terabaikan namun terbukti menjadi titik terlemah.

4. Kesimpulan

Tinjauan sistematis ini menyimpulkan adanya sebuah paradoks utama dalam keamanan 2FA, di mana seiring meningkatnya kekuatan teoretis protokol, titik kegagalan paling kritis justru bergeser pada fundamental implementasi praktis dan faktor manusia. Bukti-bukti dari literatur ilmiah selama lima tahun terakhir secara konsisten menunjukkan bahwa vektor ancaman paling dominan bukanlah pada kriptografi itu sendiri, melainkan pada kerentanan seperti penyimpanan *secret key* dalam format *plaintext* di perangkat klien dan keberhasilan serangan rekayasa sosial. Hal ini menegaskan bahwa fokus evaluasi keamanan 2FA harus diperluas dari analisis protokol ke audit implementasi di dunia nyata.

Implikasi dari temuan ini sangat jelas, di mana upaya pengamanan 2FA harus menyeimbangkan antara pengembangan protokol yang kuat dengan penegakan praktik implementasi yang aman serta program edukasi pengguna yang berkelanjutan. Berdasarkan celah yang teridentifikasi, arah penelitian di masa depan disarankan untuk berfokus pada pengembangan *tools* deteksi otomatis untuk kerentanan implementasi serta melakukan studi perbandingan mendalam terhadap metode modern yang tahan *phishing* seperti *passkeys* untuk mengukur efektivitas dan usabilitasnya.

Sebagai rekomendasi praktis, bagi pengembang, diwajibkan untuk beralih dari penyimpanan lokal sederhana ke penggunaan sistem penyimpanan kredensial terenkripsi bawaan OS (seperti Android Keystore). Bagi organisasi, perlu mempertimbangkan adopsi autentikasi berbasis perangkat keras (FIDO2) untuk akses kritikal guna memitigasi risiko *phishing* yang masih efektif terhadap OTP. Terakhir, bagi peneliti, studi masa depan disarankan untuk fokus pada pengembangan *tools* audit otomatis yang dapat mendeteksi kerentanan penyimpanan kunci pada aplikasi 2FA.

Daftar Rujukan

[1] M. F. Ayub, S. Shamshad, K. Mahmood, S. K. H. Islam, R. M. Parizi, and K. K. R. Choo, "A Provably Secure Two-Factor Authentication Scheme for USB Storage Devices," *IEEE Trans. Consum. Electron.*, vol. 66, no. 4, pp. 396–405, 2020, doi: 10.1109/TCE.2020.3035566.

[2] S. Kaur, G. Kaur, and M. Shabaz, "A secure two-factor authentication framework in cloud computing," *Secur. Commun. Networks*, vol. 2022, pp. 1–9, 2022, doi: 10.1155/2022/7540891.

[3] I. ul haq, J. Wang, and Y. Zhu, "Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks," *J. Netw. Comput. Appl.*, vol. 161, no. April, pp. 1–11, 2020, doi: 10.1016/j.jnca.2020.102660.

[4] K. Munonye and M. Péter, "Machine learning approach to vulnerability detection in OAuth 2.0 authentication and authorization flow," *Int. J. Inf. Secur.*, vol. 21, no. 2, pp. 223–237, 2022, doi: 10.1007/s10207-021-00551-w.

[5] X. Yin, J. He, Y. Guo, D. Han, K.-C. Li, and A. Castiglione, "An efficient two-factor authentication scheme based on the

Merkle tree," *Sensors*, vol. 20, no. 20, p. 5735, 2020, doi: 10.3390/s20205735.
[6] W. Bian, P. Gope, Y. Cheng, and Q. Li, "Bio-AKA: An efficient fingerprint based two factor user authentication and key agreement scheme," *Futur. Gener. Comput. Syst.*, vol. 109, pp. 45–55, 2020, doi: 10.1016/j.future.2020.03.034.
[7] Q. Wang, D. Wang, C. Cheng, and D. He, "Quantum2FA: Efficient Quantum-Resistant Two-Factor Authentication Scheme for Mobile Devices," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 1, pp. 193–208, 2023, doi: 10.1109/TDSC.2021.3129512.
[8] J. Berrios, E. Mosher, S. Benzo, C. Grajeda, and I. Baggili, "Factorizing 2FA: Forensic analysis of two-factor authentication applications," *Forensic Sci. Int. Digit. Investig.*, vol. 45, p. 301569, 2023, doi: 10.1016/j.fsidi.2023.301569.
[9] C. M. Chen, S. Liu, X. Li, S. Kumari, and L. Li, "Design and Analysis of a Provable Secure Two-Factor Authentication Protocol for Internet of Things," *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/4468301.
[10] X. Hu, C. Liu, S. Liu, J. Li, and X. Cheng, "A vulnerability in 5G authentication protocols and its countermeasure," *IEICE Trans. Inf. Syst.*, vol. E103D, no. 8, pp. 1806–1809, 2020, doi: 10.1587/transinf.2019FOL0001.
[11] G. Ali, M. A. Dida, and A. Sam, "Two-factor authentication scheme for mobile money: a review of threat models and countermeasures," *Futur. Internet*, vol. 12, no. 10, p. 160, 2020, doi: 10.3390/fi12100160.
[12] T. Fei and W. Wang, "The vulnerability and enhancement of AKA protocol for mobile authentication in LTE/5G networks," *Comput. Networks*, vol. 228, 2023, doi: 10.1016/j.comnet.2023.109685.
[13] K. Marky *et al.*, "'Nah, it's just annoying!' A deep dive into user perceptions of two-factor authentication," *ACM Trans. Comput. Interact.*, vol. 29, no. 5, pp. 1–32, 2022, doi: 10.1145/3503514.
[14] K. Hussain, N. Z. Jhanjhi, H. M. ur-Rahman, J. Hussain, and M. Hasan Islam, "Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 4, pp. 417–425, 2021, doi: 10.1016/j.jksuci.2019.01.015.
[15] M. N. Sudha, M. Rajendiran, M. Specht, K. S. Reddy, and S. Sugumaran, "A low-area design of two-factor authentication using DIES and SBI for IoT security," *J. Supercomput.*, vol. 78, no. 3, pp. 4503–4525, 2022, doi: 10.1007/s11227-021-04022-w.
[16] K. Liu *et al.*, "A robust and effective two-factor authentication (2FA) protocol based on ECC for mobile computing," *Appl. Sci.*, vol. 13, no. 7, p. 4425, 2023, doi: 10.3390/app13074425.
[17] K. Busse, S. Amft, D. Hecker, and E. von Zezschwitz, "'Get a Free Item Pack with Every Activation!,'" *I-Com*, vol. 18, no. 3, pp. 217–236, 2019, doi: 10.1515/icom-2019-0012.
[18] K. M. Quadry, A. Govardhan, and M. Misbahuddin, "Design, analysis, and implementation of a two-factor authentication scheme using graphical password," *Int. J. Comput. Netw. Inf. Secur.*, vol. 13, no. 3, pp. 39–51, 2021, doi: 10.5815/IJCNIS.2021.03.04.
[19] K. Yacouba, O. Ghizlane, and E. Said, "Securing communication 2FA using post-quantic cryptosystem: Case of QC-MDPC- McEliece Cryptosystem," *Int. J. Inf. Secur. Priv.*, vol. 14, no. 2, pp. 102–115, 2020, doi: 10.4018/IJISP.2020040106.
[20] E. M. Elshamy, A. I. Hussein, H. F. A. Hamed, M. A. Abdelghany, and H. M. Kelash, "Voice over internet protocol voicemail security system using two factor authentication and biometric prints with new efficient hybrid cryptosystem," *Multimed. Tools Appl.*, vol. 80, no. 7, pp. 9877–9893, 2021, doi: 10.1007/s11042-020-09986-0.
[21] V. Baneş, C. Ravariu, B. Appasani, and A. Srinivasulu, "A Novel Two-Factor Authentication Scheme for Increased Security in Accessing the Moodle E-Learning Platform," *Appl. Sci.*, vol. 13, no. 17, 2023, doi: 10.3390/app13179675.
[22] K. A. Kamiński, A. P. Dobrowolski, Z. Piotrowski, and P. Ścibiorek, "Enhancing Web Application Security: Advanced Biometric Voice Verification for Two-Factor Authentication," *Electron.*, vol. 12, no. 18, pp. 1–19, 2023, doi: 10.3390/electronics12183791.
[23] D. Amalfitano, M. Júnior, A. R. Fasolino, and M. Delamaro, "A GUI-based Metamorphic Testing Technique for Detecting Authentication Vulnerabilities in Android Mobile Apps," *J. Syst. Softw.*, vol. 224, no. January, p. 112364, 2025, doi: 10.1016/j.jss.2025.112364.
[24] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M. A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," *Comput. Networks*, vol. 177, p. 107333, 2020, doi: 10.1016/j.comnet.2020.107333.
[25] C. M. Chen, Z. Li, S. A. Chaudhry, and L. Li, "Attacks and Solutions for a Two-Factor Authentication Protocol for Wireless Body Area Networks," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/3116593.
[26] D. Bao and L. You, "Two-factor identity authentication scheme based on blockchain and fuzzy extractor," *Soft Comput.*, vol. 27, no. 2, pp. 1091–1103, 2023, doi: 10.1007/s00500-021-05936-6.
[27] S. Mo, W. Feng, M. Huang, S. Feng, Z. Wang, and Y. Li, "Two-factor authentication for intellectual property transactions based on improved zero-knowledge proof," *Sci. Rep.*, vol. 15, no. 1, pp. 1–15, 2025, doi: 10.1038/s41598-025-89597-7.
[28] C. Huang, B. Wang, Z. Bao, and W. Qi, "2FAKA-C/S: A Robust Two-Factor Authentication and Key Agreement Protocol for C/S Data Transmission in Federated Learning," *Appl. Sci.*, vol. 14, no. 15, 2024, doi: 10.3390/app14156664.
[29] R. Bruzgiene and K. Jurgilas, "Securing remote access to information systems of critical infrastructure using two-factor authentication," *Electron.*, vol. 10, no. 15, 2021, doi: 10.3390/electronics10151819.
[30] B. D. Deebak, "Federated Learning-Based Lightweight Two-Factor Authentication Framework with Privacy Preservation for Mobile Sink in the Social IoMT," *Electron.*, vol. 12, no. 05, 2023, doi: 10.3390/electronics12051250.
[31] F. Shohaimay and E. S. Ismail, "Improved and Provably Secure ECC-Based Two-Factor Remote Authentication Scheme with Session Key Agreement," *Mathematics*, vol. 11, no. 1, pp. 1–22, 2023, doi: 10.3390/math11010005.
[32] S. Bamashmos, N. Chilamkurti, and A. S. Shahraki, "Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in an IoT Environment," *Sensors*, vol. 24, no. 11, 2024, doi: 10.3390/s24113575.
[33] M. J. Hossain, C. Xu, C. Li, S. M. H. Mahmud, X. Zhang, and W. Li, "ICAS: Two-factor identity-concealed authentication scheme for remote-servers," *J. Syst. Archit.*, vol. 117, no. February, p. 102077, 2021, doi: 10.1016/j.sysarc.2021.102077.
[34] A. Derhab, M. Belaoued, M. Guerroumi, and F. A. Khan, "Two-Factor Mutual Authentication Offloading for Mobile Cloud Computing," *IEEE Access*, vol. 8, pp. 28956–28969, 2020, doi: 10.1109/ACCESS.2020.2971024.
[35] Y. Oren and D. Arad, "Toward Usable and Accessible Two-Factor Authentication Based on the Piezo-Gyro Channel," *IEEE Access*, vol. 10, pp. 19551–19557, 2022, doi: 10.1109/ACCESS.2022.3150519.
[36] A. A. S. Alqahtani, T. Alshayeb, M. Nabil, and A. Patooghy, "Leveraging Machine Learning for Wi-Fi-Based Environmental Continuous Two-Factor Authentication," *IEEE Access*, vol. 12, no. January, pp. 13277–13289, 2024, doi: 10.1109/ACCESS.2024.3356351.
[37] Y. Zhang, D. Han, A. Li, L. Zhang, T. Li, and Y. Zhang, "MagAuth: Secure and Usable Two-Factor Authentication With Magnetic Wrist Wearables," *IEEE Trans. Mob. Comput.*, vol. 22, no. 1, pp. 311–327, 2023, doi: 10.1109/TMC.2021.3072598.
[38] H. Zhu, W. Jin, M. Xiao, S. Murali, and M. Li, "Blinkey: A two-factor user authentication method for virtual reality devices," *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 4, no. 4, 2020, doi: 10.1145/3432217.
[39] P. V. Bhole, Z. Li, S. Bokolia, T. Oh, G. W. Tigwell, and R. L. Peiris, "Haptic2FA: Haptics-Based Accessible Two-Factor Authentication for Blind and Low Vision People," *Proc. ACM Human-Computer Interact.*, vol. 8, no. MHCI, 2024, doi: 10.1145/3676509.

DOI : https://doi.org/10.52158/h9qv3j56

[40] N. Ghose, K. Gupta, L. Lazos, M. Li, Z. Xu, and J. Li, "ZITA: Zero-Interaction Two-Factor Authentication Using Contact Traces and In-Band Proximity Verification," *IEEE Trans. Mob. Comput.*, vol. 23, no. 5, pp. 6318–6333, 2024, doi: 10.1109/TMC.2023.3321514.

[41] W. Wang, G. Li, Z. Chu, H. Li, and D. Faccio, "Two-Factor Authentication Approach Based on Behavior Patterns for Defeating Puppet Attacks," *IEEE Sens. J.*, vol. 24, no. 6, pp. 8250–8264, 2024, doi: 10.1109/JSEN.2024.3355694.

[42] Z. Yang and J. Kong, "Cue-based Two Factor Authentication," 2024, doi: 10.1016/j.cose.2024.104068.

[43] T. A. Burganova, D. R. Fakhreeva, and N. N. Fakhreev, "Method of Two-Factor Authentication of Electronic Documents Using Enhanced Encrypted Non-Certified Digital Signature with the Use of Security Token with Biometric Data," *Telfor J.*, vol. 15, no. 2, pp. 50–55, 2023, doi: 10.5937/TELFOR2302050B.

[44] S. F. Pane, D. I. Haq, and M. A. H. Siregar, "Security Analysis of Two-Factor Authentication Applications: Vulnerabilities in Data Storage and Management," 2025, doi: 10.12928/mf.v7i2.13312.

DOI : https://doi.org/10.52158/h9qv3j56