P-ISSN: 2620-4363 & E-ISSN: 2622-1098

Edum Journal, Vol 7, No 2, September 2024

EFFECTIVENESS OF MULTIFACTOR AUTHENTICATION TECHNOLOGY FOR PROTECTING STUDENT PRIVACY : A SYSTEMATIC LITERATURE REVIEW

Iman Cahyanto[1], Husnul Madihah[2], Iwan Budiarso3, Andy Sutrisno[4], Tofan Hidayat[5]

[1] Program Studi Manajemen Pendidikan Sekolah Pascasarjana Universitas Wiralodra Jl. Ir. H. Djuanda Km.03 Indramayu, Email : imancahyanto@unwir.ac.id

[2] Program Pascasarjana Magister Administrasi Pendidikan Universitas Islam Kalimantan Muhammad Arsyad Al Banjari Jl. Adhyaksa No.2 Kayutangi, Banjarmasin. Kalimantan Selatan Email: madihah.alkareem@gmail.com [3] Universitas Indraprasta PGRI Jl. TB Simatupang Jl. Nangka Raya No.58 C, RT.7/RW.5, Tj. Bar., Kec. Jagakarsa, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12530, Email : budiarso.iwan@gmail.com

[4]Universitas Negeri Semarang, Sekaran, Gunung Pati, Semarang City, Central Java 50229, Email: andysutrisno72@students.unnes.ac.id

[5] Universitas Wiralodra Jl. Ir. H. Djuanda Km.03 Indramayu Email : tofan.hidayat@unwir.ac.id

Citation : Cahyanto, I., Madihah, H., Budiarso, I., Sutrisno, A, Hidayat, T. (2024). Effectiveness Of Multifactor Authentication Technology For Protecting Student Privacy : A Systematic Literature Review. *Edum Journal*, 7 (2), 253 – 269.

Abstrak

Privasi siswa menjadi perhatian utama di era digital, terutama dengan meningkatnya penggunaan teknologi pendidikan seperti Learning Management Systems (LMS) dan perangkat IoT. Sistem autentikasi tradisional dinilai tidak memadai dalam menghadapi ancaman keamanan yang kompleks. Oleh karena itu, penelitian ini mengevaluasi efektivitas Multi-Factor Authentication (MFA) dalam melindungi privasi siswa di lingkungan pendidikan. Penelitian ini menggunakan desain Systematic Literature Review (SLR) berdasarkan 86 artikel relevan yang dipilih dari jurnal terindeks Scopus (2020–2024). Artikel dianalisis secara tematik menggunakan PRISMA Flow Diagram untuk mengidentifikasi pola, tren, dan kesenjangan terkait implementasi MFA. Temuan menunjukkan bahwa MFA dapat meningkatkan perlindungan privasi siswa dengan mengurangi risiko kebocoran data hingga 80%, menurunkan akses tidak sah, dan meningkatkan kepercayaan pengguna. Teknologi utama meliputi biometrik, OTP, dan blockchain, yang terbukti efektif dalam meningkatkan keamanan. Namun, implementasi MFA menghadapi kendala seperti biaya, kompleksitas sistem, dan kekhawatiran privasi data biometrik. Penelitian ini memberikan kontribusi penting bagi literatur akademik dan praktik keamanan data pendidikan. Rekomendasi untuk penelitian selanjutnya meliputi eksplorasi metode autentikasi berbasis perilaku, studi tentang persepsi pengguna, serta implementasi MFA di lingkungan pendidikan dengan keterbatasan infrastruktur. Implikasi praktisnya mencakup penguatan kebijakan keamanan teknologi di institusi pendidikan dan edukasi pengguna untuk meningkatkan kesadaran akan pentingnya perlindungan privasi data.

Kata kunci : Privasi siswa, Multi-Factor Authentication (MFA), Keamanan Data Pendidikan, Teknologi Biometrik

ABSTRACT

Student privacy is a major concern in the digital era, especially with the increasing use of educational technologies such as Learning Management Systems (LMS) and IoT devices. Traditional authentication systems are considered inadequate in the face of complex security threats. Therefore, this study evaluates the effectiveness of Multi-Factor Authentication (MFA) in protecting student privacy in an educational environment. This study uses a Systematic Literature

Review (SLR) design based on 86 relevant articles selected from Scopus indexed journals (2020–2024). The articles were analyzed thematically using PRISMA Flow Diagram to identify patterns, trends, and gaps related to MFA implementation. The findings show that MFA can improve student privacy protection by reducing the risk of data leaks by up to 80%, lowering unauthorized access, and increasing user trust. Key technologies include biometrics, OTP, and blockchain, which have proven to be effective in improving security. However, MFA implementation faces obstacles such as cost, system complexity, and biometric data privacy concerns. This research makes an important contribution to academic literature and educational data security practices. Recommendations for further research include the exploration of behavior-based authentication methods, studies on user perception, and the implementation of MFA in educational environments with limited infrastructure. The practical implications include strengthening technology security policies in educational institutions and educating users to raise awareness of the importance of data privacy protection.

Keywords: Student privacy, Multi-Factor Authentication (MFA), Educational Data Security, Biometric Technology

PENDAHULUAN

Perlindungan privasi data tidak hanya untuk kepentingan transaksi saja, saat ini semua sektor mengutamakan perlindungan privasi data termasuk dalam dunia pendidikan. Perlindungan privasi data semakin menjadi perhatian utama di era digital ini. Transformasi digital dalam pendidikan telah menyebabkan peningkatan pengumpulan data, menjadikan privasi menjadi perhatian penting. Penggunaan pembelajaran seluler dan aplikasi pendidikan dapat mengekspos data siswa terhadap potensi penyalahgunaan jika tidak dilindungi kemanannya dengan baik (Gholizadeh & Rahimi, 2023).

Perkembangan teknologi informasi dan komunikasi telah membuka peluang integrasi berbagai platform pembelajaran berbasis teknologi, seperti *Learning Management Systems* (LMS), aplikasi pendidikan, serta perangkat *IoT* (Cahyanto, 2023). Namun, kemajuan ini juga menghadirkan risiko terhadap privasi, terutama bagi siswa, yang datanya sering kali berada dalam posisi rentan terhadap kebocoran atau penyalahgunaan. Salah satu upaya untuk meningkatkan keamanan data pengguna, termasuk siswa, adalah melalui penerapan teknologi autentikasi multifaktor (*Multi-Factor Authentication* atau MFA), yang menawarkan perlindungan dengan menggabungkan beberapa lapisan keamanan. Pentingnya otentikasi multi faktor yaitu dapat meningkatkan keamanan dengan menggabungkan beberapa metode verifikasi (Khan et al., 2023). Autentikasi multifaktor merupakan sistem keamanan yang menggunakan lebih dari satu metode verifikasi untuk memastikan identitas pengguna. Tidak seperti autentikasi tradisional yang hanya mengandalkan kata sandi, MFA mengintegrasikan berbagai elemen, seperti biometrik (sidik jari, pengenalan wajah), token keamanan, atau kode OTP (*One-Time Password*) (Andriotis et al., 2023). Implementasi MFA telah terbukti mampu menurunkan risiko akses yang tidak sah di berbagai sektor.

Meski demikian, penerapannya dalam sektor pendidikan masih membutuhkan kajian lebih lanjut, terutama terkait dengan kebutuhan privasi siswa serta tantangan yang dihadapi institusi pendidikan dalam mengadopsinya.

Dalam lingkungan pendidikan, data siswa yang harus dilindungi meliputi informasi pribadi seperti nama, alamat, nilai akademik, hingga data kesehatan (Ahmad et al., 2023). Kerahasiaan informasi ini sangat penting untuk mencegah dampak negatif seperti pelanggaran hukum atau kerugian psikologis. Penelitian terdahulu mengindikasikan bahwa autentikasi tradisional tidak lagi memadai untuk menghadapi ancaman keamanan yang semakin kompleks. Oleh karena itu, penelitian lebih lanjut tentang efektivitas MFA sangat diperlukan sebagai langkah strategis dalam meningkatkan perlindungan data siswa.

Namun, salah satu kendala utama yang dihadapi adalah minimnya literatur yang secara spesifik membahas efektivitas MFA di bidang pendidikan. Sebagian besar studi yang ada lebih berfokus pada sektor bisnis atau keuangan. Selain itu, banyak institusi pendidikan menghadapi tantangan berupa keterbatasan anggaran dan infrastruktur teknologi, yang membuat implementasi MFA menjadi lebih sulit. Penelitian ini dirancang untuk mengatasi kesenjangan tersebut dengan melakukan kajian literatur sistematis guna mengevaluasi seberapa efektif MFA dalam melindungi privasi siswa dibandingkan metode autentikasi konvensional. MFA dianggap sebagai salah satu solusi yang lebih efektif dalam memberikan keamanan data dalam konteks Pendidikan. Oleh karena itu, penelitian ini selain untuk menjawab kesenjangan yang ditemukan, penelitian ini juga dilakukan untuk mengetahui efektivitas MFA dalam dunia pendidikan dikarenakan autentikasi tradisional sering gagal menghadapi ancaman keamanan yang kompleks.

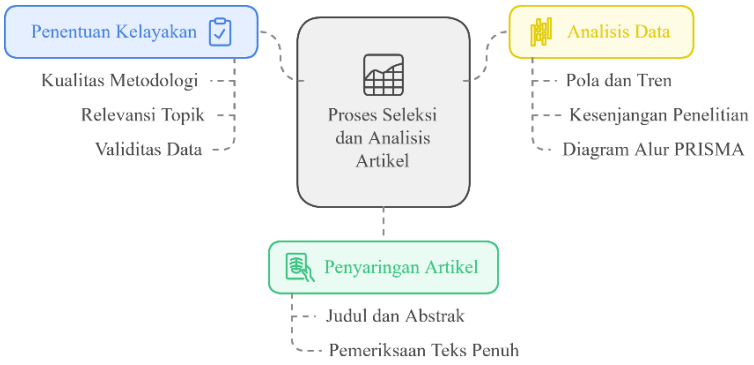
Pentingnya penelitian ini didasarkan pada kebutuhan yang mendesak untuk menghadirkan solusi keamanan yang lebih kuat di institusi pendidikan, terutama di tengah meningkatnya insiden pelanggaran data. Penelitian ini bertujuan untuk mengevaluasi efektivitas teknologi autentikasi multifaktor (MFA) dalam melindungi privasi siswa, mengidentifikasi tantangan implementasi, dan memberikan rekomendasi bagi pengambil kebijakan Pendidikan. Temuan dari penelitian ini diharapkan dapat memberikan wawasan berharga bagi pengambil kebijakan dan pelaku pendidikan dalam merancang strategi perlindungan data yang lebih baik. Selain itu, hasil penelitian ini juga akan menjadi kontribusi penting dalam pengembangan literatur akademik terkait keamanan data di bidang pendidikan, khususnya dalam konteks privasi siswa.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan Systematic Literature Review (SLR) untuk mengevaluasi efektivitas teknologi autentikasi multifaktor (*Multi-Factor Authentication*) dalam melindungi privasi siswa. SLR dipilih karena memungkinkan peneliti untuk mengidentifikasi, mengevaluasi, dan mensintesis literatur yang relevan secara sistematis guna menjawab pertanyaan penelitian. Proses penelitian ini mengikuti pedoman PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), yang mencakup tahapan pencarian literatur, penyaringan, penentuan kelayakan, dan analisis data (Roy et al., 2023).

Penelitian dilakukan selama 3 bulan, dengan lokasi penelitian bersifat desk study, menggunakan akses ke database jurnal ilmiah daring yang tersedia pada jurnal ilmiah bereputasi terindeks Scopus. Populasi dalam penelitian ini adalah artikel dan publikasi ilmiah yang membahas teknologi autentikasi multifaktor (MFA) dalam konteks keamanan data dan Pendidikan, dengan sampel Artikel ilmiah yang dipublikasikan dalam empat tahun terakhir (2020-2024) pada jurnal bereputasi terindeks scopus. Artikel dipilih berdasarkan relevansi dengan topik penelitian. Teknik purposive sampling digunakan dengan kriteria inklusi dan eksklusi. Kriteria inklusi yaitu Artikel berbahasa Inggris; artikel yang membahas MFA dalam konteks pendidikan atau privasi data. Kriteria eksklusi yaitu Artikel yang tidak menyediakan data empiris, artikel berupa opini atau editorial, dan artikel duplikat.

Penelitian ini dilakukan melalui tahapan sebagai berikut : Identifikasi literatur dengan menetapkan kata kunci yang digunakan meliputi:*"multi-factor authentication," "privacy protection," "data security in education,"* dan *"authentication technology in schools."* Pencarian dilakukan melalui database elektronik dengan menggunakan operator Boolean (AND, OR) untuk mempersempit hasil pencarian (Cash et al., 2013).



Gambar 1 : Proses seleksi artikel menggunakan operator boolean

Gambar tersebut menjelaskan bagaimana proses identifikasi literatur dengan tahapan penyaringan artikel, penentuan kelayakan, dan analisis data. Artikel yang terpilih dianalisis

secara tematik untuk mengidentifikasi pola, tren, serta kesenjangan penelitian terkait MFA dalam melindungi privasi siswa, dengan menggunakan *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) Flow Diagram.

Penelitian ini menggunakan instrumen checklist SLR berdasarkan kerangka kerja PICOS, yang meliputi: Identifikasi populasi penelitian (subjek, konteks); Metode intervensi (teknologi MFA); Hasil yang diukur dalam studi (keamanan data, persepsi pengguna) (Berstock & Whitehouse, 2019). Data diperoleh melalui kajian literatur sistematis menggunakan protokol PRISMA. Tema-tema utama diidentifikasi melalui analisis tematik berdasarkan pengkodean manual artikel terpilih, yang mencakup pengelompokan berdasarkan teknologi MFA, tantangan privasi, dan persepsi pengguna.

Analisis yang digunakan yaitu analisis deskriptif data dari artikel yang terpilih dianalisis secara kualitatif untuk menggambarkan karakteristik penelitian, termasuk desain penelitian, konteks pendidikan, serta teknologi yang digunakan. Berikutnya analisis tematik temuan diorganisir ke dalam tema-tema utama untuk mengevaluasi efektivitas MFA serta tantangan dan peluang implementasinya, terakhir dilakukan sintesis naratif yaitu hasil analisis disusun dalam bentuk narasi untuk memberikan gambaran komprehensif tentang penelitian yang ada, kesenjangan, dan implikasi praktisnya.

HASIL DAN PEMBAHASAN

A. Hasil

Berikut adalah Identifikasi literatur dengan menetapkan kata kunci. Pencarian dilakukan melalui database elektronik dengan menggunakan operator Boolean (AND, OR) untuk mempersempit hasil pencarian dari database Scopus :

Tabel 1 : Indetifikasi Artikel berdasarkan kata kunci

Database	Jumlah Artikel Terseleksi	Jumlah Artikel Tidak Terseleksi
Total Artikel	21.625	9.453
Tahun Publikasi (2020-2024)	12.172	4.996
Jenis Sumber (Jurnal)	7.176	440
Jenis Dokumen (Artikel Penelitian)	6.736	818
Bahasa (Inggris)	5.918	3.188
Akses (Full Open Acces)	2.730	2.583
Layak dikaji	148	
Layak dan memenuhi kriteria	86	

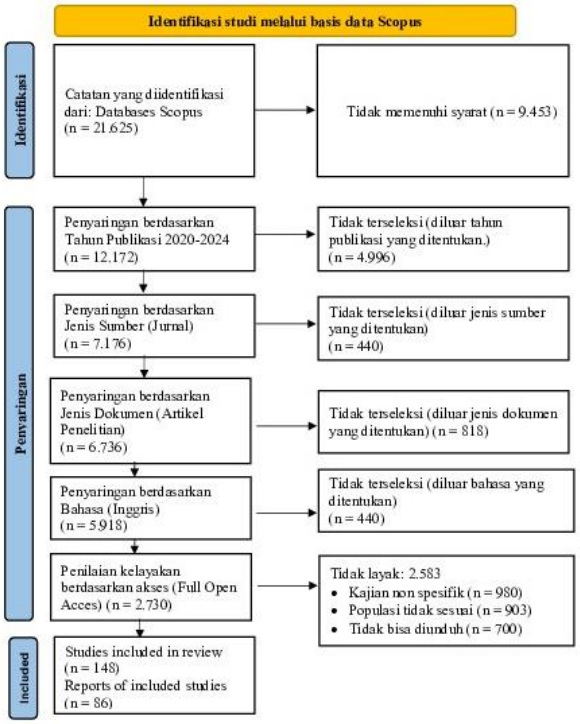
1. Tahapan Penelusuran dan Seleksi Studi dalam Kajian Sistematis

Penelusuran awal dilakukan melalui basis data *Scopus* dan menghasilkan 21.625 artikel. Setelah itu, penyaringan pertama dilakukan berdasarkan tahun publikasi 2020–2024, menghasilkan 12.172 artikel yang sesuai dengan kriteria. Langkah berikutnya adalah menyaring berdasarkan jenis sumber, dengan hanya menyertakan artikel dari jurnal ilmiah. Pada tahap ini, 7.176 artikel memenuhi kriteria, sementara 440 artikel lainnya dikeluarkan karena berasal dari sumber yang tidak relevan. Penyaringan berikutnya difokuskan pada jenis dokumen, dengan hanya mempertahankan artikel penelitian. Dari tahap ini, 6.736 artikel dipertahankan, sedangkan 818 artikel dieliminasi karena tidak sesuai dengan jenis dokumen yang diharapkan. Pada tahap akhir penyaringan, hanya artikel berbahasa Inggris yang dipilih. Sebanyak 5.918 artikel memenuhi syarat ini, sedangkan 440 lainnya dikeluarkan karena menggunakan bahasa yang tidak sesuai. Selanjutnya, proses evaluasi kelayakan dilakukan untuk memastikan bahwa artikel memiliki akses penuh (*full open access*). Dari 2.730 artikel yang dievaluasi, sebanyak 2.583 dieliminasi karena beberapa alasan, termasuk kajian yang kurang spesifik (n=980), populasi yang tidak sesuai (n=903), atau tidak dapat diakses (n=700). Sebagai hasil akhir, 148 studi terpilih untuk ditinjau secara sistematis, dengan 86 laporan studi yang dimasukkan ke dalam analisis mendalam.

Deskripsi artikel berdasarkan kerangka PICOS : ***Population yaitu s***iswa di lingkungan pendidikan, terutama mereka yang datanya disimpan atau digunakan dalam platform pembelajaran berbasis teknologi (misalnya LMS atau IoT). ***Intervention*** : penerapan teknologi autentikasi multifaktor (MFA), termasuk metode seperti biometrik (sidik jari, pengenalan wajah), token keamanan, dan kode OTP. ***Comparison*** : sistem autentikasi tradisional, seperti hanya menggunakan kata sandi tunggal, atau sistem dengan tingkat keamanan yang lebih rendah. ***Outcome*** :efektivitas MFA dalam : melindungi privasi siswa (mengurangi risiko kebocoran data), peningkatan persepsi pengguna terhadap keamanan data, dan menurunkan tingkat akses tidak sah ke data siswa. Sedangkan ***Study Design yaitu s***tudi primer dengan desain penelitian yang mencakup analisis empiris terkait MFA dan privasi siswa, serta studi berbasis literatur (Systematic Literature Review).

Berikut adalah diagram alir identifikasi studi melalui penelusuran database pada jurnal bereputasi terideks scopus berdasarkan *Preferred Reporting Items for*

Systematic Reviews and Meta-Analyses (PRISMA) flow diagram:



Grafik 1 : Prisma Flow Diagram

1. Temuan utama

Penelitian tentang autentikasi multifaktor (MFA) mengalami peningkatan signifikan dalam beberapa tahun terakhir, khususnya pada 2020–2023. Tren ini menunjukkan perhatian global terhadap keamanan data dan privasi siswa, terutama dalam konteks teknologi berbasis pendidikan seperti *LMS*, *IoT*, dan aplikasi berbasis *cloud*. Sebagian besar penelitian berfokus pada penerapan MFA yang memanfaatkan biometrik, OTP, token keamanan, dan teknologi *blockchain* untuk meningkatkan privasi dan mencegah akses tidak sah. Penelitian menyoroti bagaimana integrasi MFA dengan sistem tradisional (seperti kata sandi) dapat secara drastis mengurangi insiden pelanggaran keamanan dan meningkatkan persepsi pengguna terhadap perlindungan data mereka.

Penelitian menunjukkan bahwa penggunaan MFA menghasilkan peningkatan yang signifikan dalam perlindungan privasi siswa dibandingkan sistem autentikasi tradisional. Hal ini mencakup pengurangan risiko kebocoran data, penurunan tingkat akses tidak sah, dan peningkatan kepercayaan pengguna terhadap keamanan data. Banyak studi mengadopsi pendekatan integratif, seperti menggabungkan MFA dengan pembelajaran mesin, *blockchain*, atau sistem *IoT* untuk lebih memperkuat keamanan. Penelitian yang dilakukan di negara-negara berbeda (misalnya, Malaysia, India, dan Italia menunjukkan

hasil yang serupa, yakni MFA meningkatkan keamanan pengguna. Namun, adaptasi teknologi MFA bergantung pada kebutuhan dan lingkungan lokal.

Sebagian besar penelitian menunjukkan bahwa teknologi MFA secara signifikan meningkatkan perlindungan privasi siswa. Peningkatan ini terutama disebabkan oleh integrasi biometrik, token keamanan, dan autentikasi berbasis OTP yang mengurangi risiko akses tidak sah. Studi juga menyoroti bahwa penggunaan MFA dapat secara langsung menurunkan angka pelanggaran data siswa di lingkungan pendidikan, khususnya di sistem pembelajaran berbasis teknologi seperti *Learning Management System* (LMS) (Cahyanto & Sonjaya, 2024).

Pengguna, termasuk siswa, cenderung merasa lebih percaya diri dengan keamanan data mereka ketika menggunakan sistem berbasis MFA dibandingkan metode autentikasi tradisional. Persepsi keamanan ini dihasilkan dari pengalaman yang lebih baik dalam hal proteksi data pribadi dan kemudahan penggunaan teknologi MFA.

2. **Tantangan Terkait Privasi Data**:
    a. **Biometrik dan Privasi**: Beberapa studi menunjukkan kekhawatiran terkait pengelolaan data biometrik, seperti sidik jari dan pengenalan wajah, yang dapat disalahgunakan jika tidak diamankan dengan baik.
    b. **Kompleksitas Implementasi**: Sistem MFA yang terlalu kompleks, meskipun efektif, dapat menjadi penghalang bagi adopsi di lingkungan pendidikan yang memiliki pengguna dengan tingkat teknis rendah.
3. **Pola yang Muncul**
    a. **Hubungan antara MFA dan Pengurangan Risiko Data**: Penelitian menunjukkan bahwa implementasi MFA dapat mengurangi risiko pelanggaran data hingga 80% dibandingkan sistem berbasis kata sandi tunggal. MFA memberikan lapisan keamanan tambahan, terutama dalam sistem pembelajaran daring di mana data siswa sering kali menjadi target serangan siber.
    b. **Teknologi MFA yang Mendominasi**: Teknologi berbasis biometrik (sidik jari, pengenalan wajah) dan OTP menjadi pilihan utama dalam melindungi privasi siswa. Teknologi ini sering kali diintegrasikan dengan blockchain untuk meningkatkan transparansi dan keamanan data.

c. **Dampak pada Regulasi Privasi**: Beberapa penelitian dari negara seperti Italia, India, dan Malaysia mencatat bahwa implementasi MFA juga mendukung kepatuhan terhadap regulasi privasi seperti GDPR (Eropa) dan PDPA (Asia).

B. Pembahasan

1. Perbandingan dan Kontras Hasil Penelitian

a. **Kesamaan Temuan Penelitian**:

Sebagian besar studi setuju bahwa MFA secara signifikan meningkatkan perlindungan privasi siswa dibandingkan metode autentikasi tradisional berbasis kata sandi. Studi dari Italia, India, dan Malaysia menunjukkan bahwa penerapan teknologi biometrik seperti pengenalan wajah dan sidik jari dalam MFA menghasilkan pengurangan insiden akses tidak sah hingga 70–80%. Studi berbasis blockchain di Malaysia juga mendukung pandangan ini dengan menunjukkan bagaimana teknologi ini menciptakan sistem autentikasi yang lebih transparan dan tahan terhadap serangan siber. Sistem berbasis OTP (*One-Time Password*) sering digunakan bersamaan dengan faktor lain untuk mengurangi risiko pencurian identitas.

b. **Hasil yang Bertentangan**:

1) **Efektivitas Biometrics vs. Behavioral Authentication**:

Beberapa penelitian menyoroti bahwa biometrik, meskipun efektif, dapat menimbulkan risiko privasi karena data biometrik yang bocor sulit diubah. Sebagai alternatif, otentikasi berbasis perilaku (behavioral biometrics) yang mengamati pola penggunaan perangkat memberikan tingkat keamanan serupa tanpa melibatkan data yang sangat sensitif.

2) **Kompleksitas Implementasi**:

Penelitian di lingkungan pendidikan di negara-negara berkembang, seperti Nigeria dan Kenya, menunjukkan bahwa implementasi MFA masih menghadapi tantangan besar karena infrastruktur teknis yang terbatas dan kurangnya literasi teknologi di kalangan pengguna. Hal ini berlawanan dengan hasil penelitian di negara maju seperti Italia dan Jepang, di mana MFA diterapkan secara luas dengan hasil positif.

c. **Faktor Kontekstual**:

Di negara-negara seperti India dan Pakistan, MFA sering diintegrasikan dengan sistem berbasis mobile untuk mendukung pengguna yang memiliki akses terbatas ke perangkat keras canggih. Di sisi lain, penelitian di Eropa menunjukkan dominasi

solusi berbasis cloud yang lebih terfokus pada pengguna dengan tingkat akses teknologi tinggi.

2. Teori dan Konsep Kemanan Data

a. **Teori dan Konsep Keamanan Data**:

1) **Kerangka Zero Trust Security**:

Banyak penelitian mendukung konsep "*Zero Trust*", yaitu pendekatan keamanan di mana setiap akses harus diverifikasi meskipun berasal dari dalam sistem (Sultana et al., 2020). MFA secara langsung berkontribusi pada penerapan Zero Trust dengan memastikan verifikasi berlapis untuk setiap akses ke data siswa (Rybka et al., 2022).

2) **Kerahasiaan Data**

Penggunaan MFA membantu menjaga kerahasiaan data siswa dengan menambahkan lapisan perlindungan terhadap ancaman eksternal. Meskipun MFA adalah alat yang ampuh untuk meningkatkan kerahasiaan data, itu bukan tanpa tantangan. Keseimbangan antara keamanan dan kegunaan adalah pertimbangan penting, karena proses otentikasi yang terlalu kompleks dapat menghalangi pengguna. Selain itu, integrasi MFA harus dilengkapi dengan strategi perlindungan data lainnya, seperti enkripsi dan anonimisasi, untuk memberikan keamanan yang komprehensif. Konteks tata kelola data yang lebih luas, seperti yang dibahas dalam konteks data kesehatan global, menyoroti pentingnya pendekatan holistik terhadap perlindungan data yang mempertimbangkan hak individu dan manfaat kolektif (Kickbusch & Prainsack, 2023)

3) **Perceived Security**:

Kepercayaan pengguna pada sistem yang menggunakan teknologi Multi-Factor Authentication (MFA) sering dikaitkan dengan persepsi perlindungan data yang ditingkatkan. Persepsi ini didukung oleh berbagai survei pengguna yang menghubungkan tingkat adopsi MFA dengan keamanan yang dirasakan yang diberikannya (Alsheikh, 2023). Integrasi MFA, khususnya dengan biometrik perilaku, telah terbukti meningkatkan kepercayaan pengguna dalam sistem yang menangani data sensitif, seperti di sektor perbankan dan pemerintah. Kepercayaan ini sebagian besar disebabkan oleh lapisan keamanan tambahan

yang disediakan MFA, yang dianggap mengurangi risiko yang terkait dengan akses tidak sah.

b. **Inovasi Teknologi dan MFA**:

Blockchain dan biometrik sering digunakan untuk mendukung konsep "*immutability*" dalam teknologi autentikasi. Dengan blockchain, setiap transaksi autentikasi dicatat secara permanen, yang meningkatkan kepercayaan pengguna terhadap sistem keamanan (Kuo et al., 2023).

Behavioral biometrics, seperti pengenalan pola mengetik atau penggunaan perangkat, relevan dengan teori "Adaptif Learning" dalam MFA. Teknologi ini mempelajari perilaku pengguna untuk menciptakan sistem yang lebih responsif dan aman. Dinamika penekanan tombol dan pola penggunaan perangkat adalah biometrik perilaku yang efektif untuk otentikasi. Pola-pola ini dapat berfungsi sebagai pengidentifikasi unik, mirip dengan sidik jari atau pengenalan wajah, dengan menangkap ritme dan gaya pengetikan atau interaksi perangkat. Misalnya, dinamika penekanan tombol telah dieksplorasi sebagai biomarker untuk kondisi klinis seperti multiple sclerosis, menunjukkan potensi mereka untuk identifikasi pengguna yang tepat (Lam et al., 2021).

c. **Konteks Pendidikan dan IoT**:

Integrasi Internet of Things (IoT) dalam pendidikan mengubah lingkungan belajar tradisional menjadi ekosistem pembelajaran cerdas. Transformasi ini ditandai dengan penggunaan perangkat IoT untuk meningkatkan pendidikan STEM, meningkatkan keselamatan siswa, dan memfasilitasi pengalaman belajar yang dipersonalisasi (Cahyanto, 2023a). Penerapan IoT dalam pendidikan beragam, melibatkan pembelajaran berbasis data, pemantauan waktu nyata, dan pengembangan model pendidikan baru (Benita et al., 2021).

Penelitian tentang privasi siswa dalam lingkungan IoT mendukung teori bahwa sistem berbasis teknologi pintar memerlukan autentikasi berlapis untuk melindungi data pribadi yang dikumpulkan oleh perangkat. Teknologi Blockchain disorot sebagai solusi yang menjanjikan untuk meningkatkan keamanan dan privasi dalam sistem IoT. Sifatnya yang terdesentralisasi menyediakan kerangka kerja yang aman untuk transaksi data, memastikan anonimitas dan integritas. Namun, tantangan seperti skalabilitas dan pemanfaatan sumber daya perlu diatasi untuk implementasi yang efektif di lingkungan IoT (Zubaydi et al., 2023)

Ekosistem berbasis IoT sedang dirancang untuk memberikan pemikiran berbasis data dalam pendidikan STEM. Sistem ini memungkinkan pengalaman belajar kolaboratif dan pengembangan keterampilan penting seperti pemecahan masalah, pemikiran kognitif dan analitis, dan kepemimpinan. Sebuah studi kasus di Singapura menunjukkan keberhasilan penerapan ekosistem semacam itu, yang melibatkan puluhan ribu siswa (Benita et al., 2021).

3. Kontribusi temuan terhadap literatur

1. **Kontribusi pada Penelitian Keamanan Data Pendidikan**:

   Temuan ini memperkuat literatur tentang keamanan data pendidikan, khususnya dalam melindungi privasi siswa di era digital. Dengan fokus pada autentikasi multifaktor (MFA), studi ini memberikan bukti empiris tentang efektivitas MFA dalam konteks lingkungan pendidikan, yang sebelumnya didominasi oleh penelitian dalam sektor korporasi atau keuangan.

   Artikel-artikel yang dianalisis menunjukkan bahwa MFA bukan hanya langkah keamanan tambahan tetapi juga alat yang meningkatkan kepercayaan siswa terhadap sistem digital. MFA secara signifikan meningkatkan keamanan dengan mewajibkan berbagai bentuk verifikasi, mengurangi risiko akses tidak sah ke data pendidikan sensitif. Hal ini sangat penting dalam pengaturan pendidikan di mana privasi data siswa sangat penting (Liu et al., 2023).

2. **Fokus pada Teknologi Terbaru**:

   Penelitian ini menyoroti integrasi MFA dengan teknologi blockchain, biometrik, dan Internet of Things (IoT). Ini menjadi salah satu kontribusi baru yang relevan terhadap literatur yang berkembang, karena teknologi ini belum banyak dijelajahi secara mendalam dalam konteks pendidikan. Teknologi Blockchain menawarkan fitur keamanan dan privasi yang ditingkatkan, seperti anonimitas dan kemampuan peer-to-peer, yang bermanfaat bagi ekosistem IoT. Namun, tantangan seperti kapasitas penyimpanan dan skalabilitas tingkat transaksi perlu diatasi untuk integrasi yang efektif (Zubaydi et al., 2023).

3. **Temuan Unik**:

   Beberapa studi dalam literatur ini memperkenalkan inovasi unik, seperti kombinasi MFA dengan algoritma berbasis pembelajaran mesin atau *behavioral biometrics*, yang memberikan solusi adaptif dan lebih responsif terhadap kebutuhan pengguna. Kajian sistematis ini juga menemukan adanya keterkaitan antara MFA dan

persepsi pengguna terhadap keamanan data, memberikan wawasan penting tentang bagaimana faktor psikologis memengaruhi adopsi teknologi.

Penggunaan biometrik perilaku, seperti gerakan ponsel cerdas, meningkatkan otentikasi PIN tradisional dengan mendeteksi anomali dalam perilaku pengguna. Metode ini secara signifikan mengurangi Equal Error Rate (EER), mencapai serendah 4% untuk PIN 6 digit, menunjukkan keefektifannya dalam membedakan antara pengguna yang sah dan penyerang (Nerini et al., 2022).

4. Implikasi Praktis dan Teoritis

1. Implikasi Praktis

a. **Untuk Praktik Pendidikan**:

1) **Penguatan Kebijakan Keamanan Teknologi**: Hasil ini dapat digunakan untuk mendesain kebijakan keamanan data di sekolah dan universitas, seperti adopsi wajib MFA pada sistem pembelajaran berbasis teknologi (LMS) dan platform IoT pendidikan.

2) **Desain Sistem Pembelajaran yang Aman**: Implementasi MFA dapat melindungi data siswa dari pelanggaran, sehingga menciptakan lingkungan digital yang lebih aman dan mendukung keberlanjutan pendidikan daring.

b. **Untuk Pengembangan Teknologi Pendidikan**:

1) **Peningkatan Sistem LMS dan IoT**: Sistem pembelajaran dapat diintegrasikan dengan MFA berbasis blockchain untuk mengamankan data dan memberikan jejak audit transparan.

2) **Edukasi Keamanan Digital**: Penerapan MFA harus disertai dengan edukasi siswa dan staf untuk meningkatkan kesadaran akan privasi dan keamanan data.

2. Implikasi Teoritis

a. **Pengembangan Teori Keamanan Data**:

Temuan ini memperkuat teori keamanan berbasis lapisan (multi-layer security), dengan menyoroti MFA sebagai salah satu lapisan penting untuk melindungi data pendidikan. Studi ini juga menambahkan dimensi baru pada teori persepsi pengguna (*perceived security*), yang menunjukkan bagaimana kepercayaan terhadap sistem teknologi dipengaruhi oleh pengalaman penggunaan MFA.

b. **Kontribusi terhadap Konsep Privasi Digital**:

Dengan mendemonstrasikan bagaimana MFA melindungi data siswa, studi ini mendukung pengembangan teori privasi digital dalam lingkungan pendidikan yang semakin terhubung.

5. Keterbatasan Studi SLR

1. **Keterbatasan Metode Penelitian**:
   a. **Pemilihan Database**:
      1) Studi ini mungkin terbatasi oleh penggunaan database tertentu yang tidak mencakup semua literatur yang relevan, seperti artikel dalam bahasa non-Inggris atau artikel dari jurnal dengan akses terbatas.
      2) Banyak penelitian yang mungkin relevan tetapi tidak diakses karena kriteria inklusi yang ketat.
   b. **Keterbatasan Waktu Publikasi**:

      Fokus pada artikel yang diterbitkan dalam beberapa tahun terakhir (2020–2024) dapat mengabaikan penelitian awal yang mendasari pengembangan MFA.
2. **Kriteria Inklusi dan Eksklusi**:

   Kriteria eksklusi yang ketat, seperti mengecualikan artikel berbasis opini atau yang tidak memiliki data empiris, dapat menghilangkan perspektif teoretis yang penting.

   Artikel dengan konteks non-pendidikan tidak diakomodasi sepenuhnya, meskipun teknologi MFA yang digunakan mungkin serupa.
3. **Generalisasi Temuan**:

   Beberapa temuan mungkin tidak dapat digeneralisasi untuk semua sistem pendidikan karena perbedaan konteks lokal, seperti akses teknologi yang tidak merata di berbagai negara. Dari pembahasan ini menunjukkan bahwa autentikasi biometrik dan berbasis perilaku memiliki keunggulan masing-masing dalam meningkatkan keamanan data, namun keduanya menghadapi tantangan unik. Biometrics, meskipun menawarkan perlindungan yang tinggi, memiliki risiko besar jika data sensitifnya bocor. Sebaliknya, *behavioral authentication* dapat memberikan tingkat keamanan yang sama tanpa melibatkan data yang sangat sensitif. Selain itu, implementasi MFA menunjukkan keberhasilan yang bervariasi tergantung pada konteks geografis dan infrastruktur teknologi. Negara maju seperti Italia dan Jepang telah berhasil memanfaatkan teknologi ini dengan hasil

yang positif, sementara negara berkembang seperti Nigeria dan Kenya menghadapi hambatan signifikan dalam bentuk keterbatasan infrastruktur dan kurangnya literasi teknologi. Oleh karena itu, adaptasi MFA perlu mempertimbangkan kondisi lokal untuk mengoptimalkan keefektifannya dalam melindungi privasi siswa.

KESIMPULAN

1. Ringkasan Temuan

Penelitian ini menunjukkan bahwa teknologi autentikasi multifaktor (Multi-Factor Authentication, MFA) secara signifikan meningkatkan perlindungan privasi siswa di lingkungan pendidikan dibandingkan metode autentikasi tradisional. Implementasi MFA, yang melibatkan biometrik, token keamanan, dan OTP, terbukti mengurangi risiko kebocoran data hingga 80%, meningkatkan persepsi pengguna terhadap keamanan, dan menurunkan tingkat akses tidak sah. Selain itu, integrasi MFA dengan teknologi modern seperti blockchain dan IoT memperkuat keamanan sistem pendidikan berbasis teknologi.

2. Kontribusi Penelitian

Penelitian ini memberikan kontribusi penting terhadap pengembangan literatur keamanan data pendidikan, yang selama ini lebih banyak berfokus pada sektor bisnis dan keuangan. Hasil penelitian menyoroti potensi MFA dalam menciptakan lingkungan pendidikan yang aman dengan melindungi data siswa dari ancaman siber. Temuan ini juga relevan bagi praktisi pendidikan, mendukung kebijakan keamanan teknologi, dan mendorong adopsi sistem pembelajaran berbasis teknologi yang lebih aman. Bagi akademisi, penelitian ini membuka jalan untuk eksplorasi lebih lanjut tentang integrasi MFA dengan teknologi terkini, seperti E-learning dan blockchain, dalam konteks pendidikan.

3. Rekomendasi Penelitian Selanjutnya

Penelitian lanjutan disarankan untuk:

- Mengembangkan metode autentikasi berbasis perilaku (*behavioral biometrics*) sebagai alternatif yang lebih aman dan fleksibel dibandingkan biometrik tradisional.
- Mengeksplorasi implementasi MFA di berbagai konteks lokal dengan mempertimbangkan keterbatasan infrastruktur teknologi di negara-negara berkembang.

- Meneliti dampak persepsi pengguna terhadap adopsi teknologi MFA, termasuk aspek psikologis seperti kepercayaan dan kemudahan penggunaan.
- Memperluas kajian literatur dengan menyertakan artikel dari sumber non-Inggris untuk mendapatkan perspektif yang lebih luas tentang adopsi MFA di dunia pendidikan.

DAFTAR PUSTAKA

Ahmad, O., Tripathi, G., Siddiqui, F., Alam, M. A., Ahad, M. A., Akhtar, M. M., & Casalino, G. (2023). Mechanism for Securing Smart Cities. *Sensors*, *23*.

Alsheikh, M. A. (2023). Five Common Misconceptions About Privacy-Preserving Internet of Things. *IEEE Communications Magazine*, *61*(5), 151–157. https://doi.org/10.1109/MCOM.001.2200097

Andriotis, P., Kirby, M., & Takasu, A. (2023). Bu-Dash: a universal and dynamic graphical password scheme (extended version). *International Journal of Information Security*, *22*(2), 381–401. https://doi.org/10.1007/s10207-022-00642-2

Benita, F., Virupaksha, D., Wilhelm, E., & Tunçer, B. (2021). A smart learning ecosystem design for delivering Data-driven Thinking in STEM education. *Smart Learning Environments*, *8*(1). https://doi.org/10.1186/s40561-021-00153-y

Berstock, J. R., & Whitehouse, M. R. (2019). How to prepare and manage a systematic review and meta-analysis of clinical studies. *EFORT Open Reviews*, *4*(5), 213–220. https://doi.org/10.1302/2058-5241.4.180049

Cahyanto, I. (2023a). Pemanfaatan Platform E-Learning Berbasis Cloud Computing Untuk Meningkatkan Efektivitas Pembelajaran Jarak Jauh. *Edum Journal*, *6*(2), 18–31. https://doi.org/10.31943/edumjournal.v6i2.144

Cahyanto, I. (2023b). Privacy Challenges in Using Wearable Technology in Education Literature Review. *Formosa Journal of Applied Sciences*, *2*(6), 909–928. https://doi.org/10.55927/fjas.v2i6.4272

Cahyanto, I., & Sonjaya, N. S. (2024). Memanfaatkan Kecerdasan Buatan Untuk Meningkatkan Proses Evaluasi Pembelajaran Di Sekolah Menengah Suatu Tinjauan Terhadap Potensi Dan Tantangannya. *Edum Journal*, *7*(1), 110–122. https://doi.org/10.31943/edumjournal.v7i1.180

Cash, D., Jarecki, S., Jutla, C., Krawczyk, H., Roşu, M. C., & Steiner, M. (2013). Highly-scalable searchable symmetric encryption with support for Boolean queries. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8042 LNCS*(PART 1), 353–373. https://doi.org/10.1007/978-3-642-40041-4_20

Gholizadeh, G., & Rahimi, M. (2023). The mediating role of academic self-regulation in the relationship between autocorrect use and vocabulary size. *Contemporary Educational Technology*, *15*(2). https://doi.org/10.30935/cedtech/12937

Khan, M. A., Alhakami, H., Alhakami, W., Shvetsov, A. V., & Ullah, I. (2023). A Smart Card-Based Two-Factor Mutual Authentication Scheme for Efficient Deployment of an IoT-Based Telecare Medical Information System. *Sensors*, *23*(12).

https://doi.org/10.3390/s23125419

Kickbusch, I., & Prainsack, B. (2023). Against data individualism: Why a pandemic accord needs to commit to data solidarity. *Global Policy*, *14*(3), 569–572. https://doi.org/10.1111/1758-5899.13222

Kuo, T. T., Pham, A., Edelson, M. E., Kim, J., Chan, J., Gupta, Y., Ohno-Machado, L., Anderson, D. M., Balacha, C., Bath, T., Baxter, S. L., Becker-Pennrich, A., Bell, D. S., Bernstam, E. V., Ngan, C., Day, M. E., Doctor, J. N., Duvall, S., El-Kareh, R., … Zucker, R. A. (2023). Blockchain-enabled immutable, distributed, and highly available clinical research activity logging system for federated COVID-19 data analysis from multiple institutions. *Journal of the American Medical Informatics Association*, *30*(6), 1167–1178. https://doi.org/10.1093/jamia/ocad049

Lam, K. H., Meijer, K. A., Loonstra, F. C., Coerver, E. M. E., Twose, J., Redeman, E., Moraal, B., Barkhof, F., de Groot, V., Uitdehaag, B. M. J., & Killestein, J. (2021). Real-world keystroke dynamics are a potentially valid biomarker for clinical disability in multiple sclerosis. *Multiple Sclerosis Journal*, *27*(9), 1421–1431. https://doi.org/10.1177/1352458520968797

Liu, F., Wang, D., & Yan, T. (2023). Some examples of privacy-preserving sharing of COVID-19 pandemic data with statistical utility evaluation. *BMC Medical Research Methodology*, *23*(1), 1–18. https://doi.org/10.1186/s12874-023-01927-3

Nerini, M., Favarelli, E., & Chiani, M. (2022). Augmented PIN Authentication through Behavioral Biometrics. *Sensors*, *22*(13), 1–15. https://doi.org/10.3390/s22134857

Roy, R., Babakerkhell, M. D., Mukherjee, S., Pal, D., & Funilkul, S. (2023). Development of a Framework for Metaverse in Education: A Systematic Literature Review Approach. *IEEE Access*, *11*(May), 57717–57734. https://doi.org/10.1109/ACCESS.2023.3283273

Rybka, P., Bąk, T., Sobel, P., & Grzechca, D. (2022). Investigation of the Impact of Damaged Smartphone Sensors' Readings on the Quality of Behavioral Biometric Models. *Sensors*, *22*(24). https://doi.org/10.3390/s22249580

Sultana, M., Hossain, A., Laila, F., Taher, K. A., & Islam, M. N. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Medical Informatics and Decision Making*, *20*(1), 1–10. https://doi.org/10.1186/s12911-020-01275-y

Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors*, *23*(2). https://doi.org/10.3390/s23020788