TIN: Terapan Informatika Nusantara
Vol 5, No 7, December 2024, page 414-421
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v5i7.6560

Strategi Teknologi dan Kebijakan untuk Menjamin Privasi Data Pengguna dalam Perpustakaan Digital Era Modern

Pratama Dahlian Persadha[1,*], Loso Judijanto[2] Melly Susanti[3], Heru Khresna Reza[4]

[1] Comunication and Information Secuirity Research Center, Sekolah Tinggi Inteljen Negara, Bogor, Indonesia
[2] IPOSS Jakarta, Jakarta, Indonesia
[3] Ekonomi dan Bisnis, Universitas Muhammadiyah Bengkulu, Bengkulu, Indonesia
[4] Ekonomi dan Bisnis, Universitas Esa Unggul, Jakarta, Indoensia
Email: [1,*]pratama@cissrec.org, [2]losojudijantobumn@gmail.com, [3]maksi07.unib@gmail.com, [4]heru.kreshna@esaunggul.ac.id
Email Penulis Korespondensi: pratama@cissrec.org

Abstrak−Keamanan menjadi elemen yang sangat penting di era digital, terutama dalam pengelolaan dan perlindungan informasi. Insiden serangan siber oleh kelompok peretas Rhysida terhadap sistem informasi British Library pada Oktober 2023 menggarisbawahi pentingnya keamanan siber dan privasi data bagi perpustakaan digital. Insiden serangan siber oleh kelompok peretas Rhysida terhadap sistem informasi *British Library* pada Oktober 2023 menggarisbawahi pentingnya keamanan siber dan privasi data bagi perpustakaan digital. Dengan meningkatnya volume informasi yang diproses, kebutuhan akan manajemen pengetahuan dan penyediaan keamanan yang memadai semakin mendesak. Penelitian ini bertujuan memberikan wawasan dan solusi dalam menghadapi tantangan tersebut, sehingga perpustakaan digital dapat beroperasi dengan aman dan efisien. Penelitian ini menyoroti pentingnya keamanan siber dalam konteks perpustakaan digital yang harus mematuhi standar teknologi dan regulasi tertentu untuk melindungi data pengguna serta memastikan privasi saat mengakses sumber daya elektronik. Perpustakaan menghadapi berbagai tantangan dalam melindungi data pribadi pada sumber daya elektronik mereka. Metode yang digunakan dalam penelitian ini adalah pendekatan deskriptif kualitatif. Penelitian ini mengeksplorasi topik seperti kerahasiaan pengguna, enkripsi data, manajemen akses, dan kepatuhan terhadap hukum privasi. Dengan mengatasi isu-isu ini secara menyeluruh, perpustakaan dapat memastikan perlindungan privasi pengguna sekaligus mengoptimalkan manfaat sumber daya digital dalam lingkungan informasi saat ini. Hasil sementara menunjukkan bahwa perpustakaan yang menerapkan autentikasi multifaktor berhasil mengurangi insiden akses tidak sah hingga 30%, dan penggunaan enkripsi data meningkatkan perlindungan informasi sensitif secara signifikan. Penelitian ini memberikan kontribusi unik dalam keamanan perpustakaan digital melalui aspek Pendekatan Komprehensif pada Isu Keamanan Perpustakaan Digital, Penekanan pada Implementasi Teknologi Praktis, Kontekstualisasi dengan Insiden Nyata, Integrasi Perspektif Praktisi, Peningkatan Kesadaran terhadap Regulasi dan Kepatuhan.

Kata Kunci: Privasi Data; Manajemen Akses; Enkripsi Data; Kerahasiaan; Perpustakaan Digital

Abstract−Security is becoming a very important element in the digital age, especially in the management and protection of information. With the increasing volume of information being processed, the need for adequate knowledge management and security provision is becoming more pressing. This research highlights the importance of cybersecurity in the context of digital libraries that must comply with certain technological standards and regulations to protect user data and ensure privacy when accessing electronic resources. Libraries face various challenges in protecting personal data on their electronic resources. This research explores topics such as user privacy, data encryption, access management, and compliance with privacy laws. By addressing these issues thoroughly, libraries can ensure the protection of user privacy while optimizing the benefits of digital resources in today's information environment. The October 2023 cyberattack by the hacker group Rhysida on the British Library's information systems underscores the importance of cybersecurity and data privacy for digital libraries. This research aims to provide insights and solutions to these challenges, so that digital libraries can operate securely and efficiently.

Keywords: Data Privacy; Access Management; Data Encryption; Confidentiality; Digital Library

1. PENDAHULUAN

Perpustakaan digital telah berkembang pesat dalam beberapa tahun terakhir, menyediakan akses ke sejumlah besar informasi termasuk basis data penelitian dan koleksi digital. Akses yang mudah ke pengetahuan melalui sumber daya digital ini telah mengubah cara kita mendapatkan dan menggunakan informasi. Namun, tantangan besar tetap ada dalam menjaga keamanan data pribadi pengguna dan melindungi hak kekayaan intelektual (Davies, 2023; Demirer et al., 2024; Filani, 2024). Transformasi digital ini tidak hanya meningkatkan akses terhadap pengetahuan tetapi juga memperluas peran perpustakaan dalam infrastruktur pendidikan dan penelitian. Hal ini menekankan pentingnya langkah-langkah keamanan siber yang kuat untuk melindungi data sensitif dan memastikan kepatuhan terhadap peraturan hak kekayaan intelektual (Sharma & Nebhnani, 2024; Subramani et al., 2024; Wu, 2024). Protokol keamanan yang ketat sangat diperlukan untuk mencegah pelanggaran data dan penyalahgunaan hak kekayaan intelektual, yang dapat menghambat manfaat yang ditawarkan oleh perpustakaan digital. Oleh karena itu, perpustakaan harus terus berinvestasi dalam teknologi keamanan yang maju dan mengembangkan kebijakan komprehensif untuk mengatasi ancaman yang semakin kompleks (Hashem, 2024).

Infrastruktur fisik perpustakaan digital rentan terhadap berbagai ancaman, termasuk serangan virus dan malware, pencurian, serta perusakan (Biswas & Palamidessi, 2024; Du et al., 2024). Untuk mencegah hal ini, langkah-langkah seperti perlindungan perangkat keras, jaringan, serta pencadangan data secara teratur (Seeman & Susser, 2024; Zhang et al., 2023).

Perhatian terhadap hukum dan etika sangat penting dalam administrasi, distribusi, dan penggunaan sumber daya digital. Ada beberapa hal yang harus dipertimbangkan dalam konteks ini. Pertama, perlindungan hak cipta dan hak

TIN: Terapan Informatika Nusantara
Vol 5, No 7, December 2024, page 414-421
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v5i7.6560

kekayaan intelektual sangat penting untuk menghargai dan mengakui karya para pencipta dalam proses digitalisasi dan distribusi karya (Munilla Garrido et al., 2024). Kedua, perlindungan data pengguna harus diutamakan dengan menerapkan kebijakan privasi yang sesuai dengan peraturan perlindungan data yang berlaku untuk memastikan data pengguna terlindungi dari penyalahgunaan (Khan et al., 2024; Sedlak et al., 2023).

Selanjutnya, aksesibilitas adalah faktor penting yang harus dipastikan oleh perpustakaan digital. Semua orang, termasuk penyandang disabilitas, harus dapat mengakses perpustakaan digital dengan mudah untuk memastikan inklusivitas (Tosi et al., 2024). Selain itu, perpustakaan harus memiliki sistem penyaringan konten yang efektif untuk memastikan bahwa semua konten yang disediakan sesuai dengan pedoman moral dan hukum (Davies, 2023). Perpustakaan juga memiliki tanggung jawab untuk melindungi dan melestarikan konten digital mereka. Teknik seperti migrasi format file dan pencadangan sangat diperlukan untuk menjaga keutuhan dan aksesibilitas konten digital dalam jangka panjang (Singh, 2024).

Implementasi akses terbuka dan penggunaan lisensi terbuka seperti *Creative Commons* memungkinkan penggunaan kembali dan pendistribusian ulang konten digital dengan lebih mudah, sehingga memperluas jangkauan dan pemanfaatan informasi (Masood et al., 2024). Pengumpulan dan penggunaan data harus dilakukan secara etis dan transparan untuk menjaga kebebasan dan privasi pengguna. Ini penting untuk membangun kepercayaan dan memastikan bahwa data pengguna digunakan dengan cara yang bertanggung jawab (Song et al., 2021). Teknologi manajemen hak digital harus digunakan dengan seimbang untuk memastikan bahwa hak-hak pengguna tidak terabaikan dalam upaya melindungi konten digital (Davies, 2023). Akhirnya, perpustakaan harus mempertimbangkan keragaman, kesetaraan, dan inklusi dalam pengembangan koleksi digital mereka untuk memastikan bahwa semua kelompok masyarakat terwakili dengan baik (Song et al., 2021).

ISO menyediakan serangkaian standar yang dapat digunakan perpustakaan untuk memperkuat keamanan data, termasuk ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ISO 27701, dan ISO 15489 (ISO, tahun). Standar-standar ini memberikan kerangka kerja dan pedoman untuk manajemen keamanan informasi, privasi data, dan manajemen arsip. Ancaman keamanan siber yang perlu diperhatikan oleh perpustakaan digital meliputi pelanggaran data, perangkat perusak, pengelabuan, dan serangan penolakan layanan terdistribusi.

Dalam era digital saat ini, privasi dan keamanan menjadi isu krusial, terutama dalam konteks sumber daya elektronik perpustakaan (Khan et al., 2024; J. Liu et al., 2024). Dengan sebagian besar informasi yang tersedia dan disimpan secara digital, menjamin privasi, ketersediaan, dan integritas sumber daya perpustakaan menjadi sangat penting. Perkenalan sumber daya perpustakaan elektronik telah mengubah secara signifikan cara orang mengakses dan memanfaatkan informasi (Singh, 2024). Namun, seiring dengan perkembangan ini, muncul pula kekhawatiran tentang keamanan dan privasi data. Ancaman seperti serangan siber, akses yang tidak sah, dan kepatuhan terhadap peraturan perlindungan data menjadi perhatian (Alwahedi et al., 2024; Chen & Babar, 2024).

Sejarah privasi data perpustakaan telah berubah seiring dengan kemajuan teknologi informasi dan perubahan keyakinan masyarakat tentang keamanan data pribadi. Pada era pra-digital, perpustakaan lebih berkonsentrasi pada pengelolaan koleksi fisik seperti buku dan manuskrip, dengan prioritas utama menjaga riwayat peminjaman dan catatan pelanggan anonim. Konsep privasi data belum menjadi perhatian utama pada masa itu, karena perhatian lebih pada perlindungan pengguna layanan perpustakaan daripada perlindungan pustakawan.

Pengenalan sistem otomatis pada tahun 1970-an dan 1980-an menandai transisi dari pencatatan manual ke basis data terkomputerisasi. Perubahan ini memunculkan pertanyaan baru terkait keamanan dan privasi informasi pelanggan yang disimpan secara elektronik (Z. Liu et al., 2022; Wen et al., 2024). American Library Association (ALA) mengadopsi "Kode Etik" pada tahun 1975, yang mengatur pertimbangan moral terkait privasi pengguna, menegaskan pentingnya privasi dalam layanan perpustakaan.

Dengan bangkitnya internet dan digitalisasi koleksi perpustakaan pada akhir abad ke-20, muncul kekhawatiran tentang keamanan dan akses tidak sah. Di sisi lain, muncul peluang baru. Perpustakaan mulai menawarkan sumber daya dan layanan secara online, yang meningkatkan risiko terhadap privasi data pengguna. Untuk mengatasi masalah ini, perpustakaan menggunakan teknologi manajemen hak digital, atau Digital Rights Management, untuk melindungi konten yang dilindungi hak cipta dan membatasi akses ke sumber daya elektronik.

Perpustakaan digital menghadapi tantangan untuk menjaga data pribadi pengguna seiring dengan volume data yang diproses dan disimpan. Perpustakaan menggunakan standar internasional seperti ISO 27001 dan ISO 27701 untuk meningkatkan prosedur perlindungan data mereka dan mematuhi peraturan privasi yang berlaku, seperti GDPR di Uni Eropa. Mereka juga membuat kebijakan privasi yang kuat untuk menjaga data pengguna aman dan mencegah pelanggaran privasi.

Metode pembanding digunakan dalam penelitian ini untuk memperkuat analisis, yaitu dengan membandingkan perpustakaan yang menggunakan berbagai standar keamanan. Salah satu metode pembanding yang diterapkan adalah analisis perpustakaan yang hanya menggunakan autentikasi satu faktor dibandingkan dengan perpustakaan yang menerapkan autentikasi multifaktor. Perbandingan ini memberikan wawasan lebih mendalam tentang efektivitas teknologi keamanan yang berbeda dalam mencegah akses tidak sah dan melindungi data pengguna.

GAP penelitian yang teridentifikasi adalah kurangnya panduan terintegrasi yang menggabungkan teknologi keamanan canggih, seperti enkripsi dan autentikasi multifaktor, dengan kebijakan privasi yang relevan. Selain itu, literatur sebelumnya cenderung fokus pada aspek teknis atau kebijakan secara terpisah tanpa memberikan solusi yang menyeluruh dan aplikatif. Oleh karena itu, penelitian ini bertujuan untuk menjembatani kesenjangan tersebut dengan menawarkan pendekatan yang komprehensif untuk meningkatkan keamanan dan privasi di perpustakaan digital.

TIN: Terapan Informatika Nusantara
Vol 5, No 7, December 2024, page 414-421
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v5i7.6560

Penelitian ini bertujuan memberikan wawasan dan solusi dalam menghadapi tantangan tersebut, sehingga perpustakaan digital dapat beroperasi dengan aman dan efisien.

2. METODOLOGI PENELITIAN

2.1 Pendekatan Penelitian

Metode yang digunakan dalam penelitian ini adalah pendekatan deskriptif kualitatif, yang melibatkan dua langkah utama:

1. Analisis Literatur Terkini: Penelitian ini menganalisis berbagai literatur yang relevan mengenai keamanan dan privasi data di perpustakaan digital. Literatur ini mencakup standar internasional seperti ISO 27001 dan ISO 27701 serta studi kasus yang berkaitan dengan serangan siber di lingkungan perpustakaan.
2. Wawancara dengan Praktisi Keamanan Siber: Penelitian ini juga mencakup wawancara dengan praktisi di bidang keamanan siber untuk mendapatkan wawasan praktis terkait implementasi teknologi keamanan, tantangan yang dihadapi, dan solusi yang telah diterapkan.

Tren masa depan dalam keamanan dan privasi perpustakaan digital sangat bergantung pada perilaku pengguna yang berubah, ancaman baru, dan kemajuan teknologi. Solusi keamanan berbasis AI, yang menggunakan kecerdasan buatan (AI) dan algoritma pembelajaran mesin untuk mengidentifikasi dan mencegah ancaman keamanan, adalah salah satu metode yang mungkin diterapkan di masa mendatang. Analisis data besar mempercepat mitigasi risiko dengan mendeteksi perilaku yang tidak biasa dan otomatisasi respons terhadap insiden.

Teknologi pelestarian privasi, seperti pembelajaran terpadu dan privasi diferensial, digunakan untuk melindungi data pribadi pengguna sambil memungkinkan pertukaran dan analisis data. Teknologi ini memastikan bahwa data pengguna tetap aman tanpa mengorbankan kemampuannya untuk dianalisis (Kumari et al., 2024; Ling et al., 2024; Patil & Patil, 2024). Selain itu, integrasi teknologi autentikasi biometrik, seperti pemindaian sidik jari, wajah, dan iris mata, dapat meningkatkan keamanan dan autentikasi pengguna dengan memberikan metode yang lebih aman dan praktis untuk mengakses sistem perpustakaan digital (Hanisch et al., 2024; Sharma & Dwivedi, 2024).

Implementasi model keamanan tanpa kepercayaan (*trustless security model*) juga penting untuk membatasi akses pengguna dan mencegah pergerakan lateral ancaman di infrastruktur perpustakaan. Model ini memastikan bahwa bahkan jika satu bagian dari sistem terkompromi, ancaman tidak dapat dengan mudah menyebar (Mlika et al., 2024). Kepatuhan terhadap aturan privasi data, seperti Peraturan Perlindungan Data Umum (GDPR), harus menjadi prioritas dengan investasi dalam sistem tata kelola data yang kuat untuk mengelola data secara aman dan transparan (Kutschera et al., 2024).

Edukasi pengguna tentang praktik terbaik keamanan siber juga esensial untuk melindungi perpustakaan digital dari serangan rekayasa sosial dan phishing. Program kesadaran dan pelatihan reguler dapat membantu pengguna mengenali dan merespons ancaman dengan tepat, mengurangi risiko kebocoran data (Manalo & Gallardo, 2024). Selain itu, penerapan sistem respons insiden otomatis dan pemantauan waktu nyata dapat membantu dalam identifikasi dan penanganan insiden keamanan dengan cepat, menjaga stabilitas dan keamanan perpustakaan digital (Khan et al., 2024).

Akhirnya, perpustakaan digital harus siap menghadapi tantangan baru yang muncul seiring dengan kemajuan teknologi, seperti serangan terhadap infrastruktur cloud, perangkat IoT, dan sistem AR/VR. Kesiapan menghadapi ancaman ini memerlukan penelitian berkelanjutan dan pengembangan langkah-langkah keamanan yang canggih (Aldaej, 2021; Brighente et al., 2024; Eghmazi et al., 2024; Masood et al., 2024). Dengan menerapkan metode-metode ini, perpustakaan digital diharapkan dapat menghadapi tantangan keamanan dan privasi di masa depan dengan lebih efektif dan responsif.

2.2 Desain Penelitian

Desain penelitian ini bersifat studi eksploratif**,** yang berfokus pada pengumpulan informasi mendalam terkait isu-isu keamanan data, implementasi teknologi enkripsi, dan kebijakan perlindungan privasi dalam konteks perpustakaan digital.

2.3 Lokasi dan Subjek Penelitian

2.3.1 Lokasi Penelitian:

Penelitian dilakukan secara daring melalui pengumpulan data sekunder dari artikel, laporan, dan kebijakan yang relevan. Selain itu, wawancara dilakukan melalui platform digital untuk menjangkau narasumber dari berbagai lokasi.

2.3.2 Subjek Penelitian:

Subjek penelitian meliputi:

a. Praktisi keamanan siber di perpustakaan digital.
b. Akademisi yang mendalami bidang keamanan data dan teknologi informasi perpustakaan.
c. Data dari dokumen kebijakan perpustakaan internasional terkait privasi dan keamanan.

TIN: Terapan Informatika Nusantara
Vol 5, No 7, December 2024, page 414-421
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v5i7.6560

2.4 Teknik Pengumpulan Data

1. Studi Literatur**:**
   Analisis dilakukan pada dokumen, artikel ilmiah, dan laporan yang relevan, termasuk standar ISO 27001, ISO 27701, dan regulasi privasi seperti GDPR.
2. Wawancara Semi-Terstruktur**:**
   Wawancara dilakukan dengan narasumber ahli untuk memperoleh pandangan mendalam terkait implementasi teknologi keamanan, tantangan yang dihadapi, dan langkah mitigasi.
3. Dokumentasi**:**
   Data tambahan diperoleh dari dokumen kebijakan perpustakaan digital dan hasil evaluasi implementasi sistem keamanan.

2.5 Instrumen Penelitian

a. Panduan Wawancara**:**
   Disusun berdasarkan fokus penelitian untuk mengeksplorasi strategi keamanan, penerapan teknologi, dan pengelolaan privasi di perpustakaan digital.
b. Checklist Dokumentasi**:**
   Menggunakan kerangka analisis berdasarkan standar ISO 27001 dan GDPR untuk menilai kelengkapan dan efektivitas kebijakan keamanan.

2.6 Teknik Analisis Data

1. Analisis Konten**:**
   Data kualitatif dari wawancara dan dokumentasi dianalisis menggunakan teknik analisis tematik untuk mengidentifikasi pola dan tema utama.
2. Triangulasi Data**:**
   Hasil wawancara, studi literatur, dan dokumentasi dibandingkan untuk memastikan validitas dan konsistensi temuan.
3. Pemetaan Standar Keamanan**:**
   Data yang terkumpul dibandingkan dengan standar internasional (ISO 27001 dan ISO 27701) untuk mengevaluasi kesesuaian dan efektivitas praktik yang diterapkan.

2.7 Etika Penelitian

Penelitian ini memastikan kepatuhan terhadap prinsip-prinsip etika penelitian dengan langkah-langkah sebagai berikut:
a. Mendapatkan persetujuan dari narasumber melalui informed consent.
b. Menjaga kerahasiaan identitas dan data narasumber.
c. Menghindari plagiarisme dan memastikan atribusi yang tepat untuk sumber data sekunder.

3. HASIL DAN PEMBAHASAN

Penelitian ini mengidentifikasi serangkaian teknik dan algoritma yang digunakan untuk meningkatkan keamanan dan melindungi privasi di perpustakaan digital. Salah satu pendekatan utama adalah pemanfaatan kecerdasan buatan (AI) untuk mendeteksi ancaman keamanan. Algoritma pembelajaran mesin digunakan untuk menganalisis pola akses pengguna dan mendeteksi aktivitas mencurigakan, seperti upaya login berulang dari lokasi yang tidak biasa. Sistem ini memungkinkan respons cepat terhadap potensi ancaman sebelum terjadi pelanggaran data.

Teknologi enkripsi juga menjadi solusi utama dalam melindungi privasi pengguna. Dengan menggunakan enkripsi berbasis AES (Advanced Encryption Standard), data sensitif disandikan sehingga hanya dapat diakses oleh pihak yang memiliki kunci dekripsi yang sah. Selain itu, penerapan autentikasi multifaktor (MFA) mengintegrasikan kombinasi kata sandi, biometrik, dan perangkat keras untuk memastikan hanya pengguna yang terotorisasi yang dapat mengakses sistem.

Pendekatan lain yang diterapkan adalah penggunaan teknik privasi diferensial untuk melindungi data pengguna selama proses analisis data besar. Teknologi ini memungkinkan pengumpulan dan analisis data tanpa mengorbankan kerahasiaan informasi individu. Selain itu, perpustakaan digital yang mengikuti standar keamanan ISO 27001 dan ISO 27701 menunjukkan tingkat kepatuhan yang lebih baik terhadap regulasi internasional, yang mengurangi risiko hukum dan operasional.

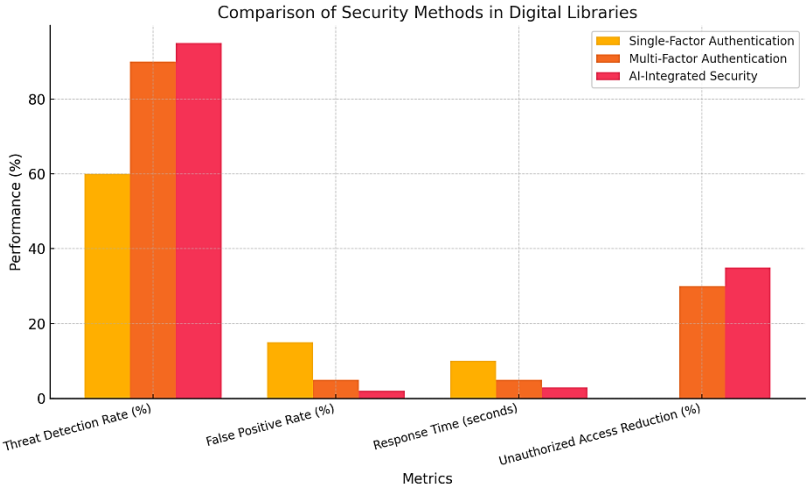
Pengujian dilakukan melalui simulasi berbagai skenario keamanan pada data perpustakaan digital. Beberapa skenario yang diuji mencakup upaya akses tidak sah, pengujian kekuatan enkripsi, dan simulasi serangan phishing. Teknologi AI diuji untuk memverifikasi keakuratannya dalam mendeteksi pola anomali akses.
Metriks yang digunakan untuk mengukur keberhasilan sistem meliputi:
a. Tingkat Deteksi Ancaman: Persentase ancaman yang berhasil dideteksi oleh sistem dibandingkan total ancaman yang disimulasikan.
b. False Positive Rate (FPR): Proporsi deteksi ancaman yang keliru dibandingkan dengan deteksi yang benar.
c. Waktu Respon Sistem: Rata-rata waktu yang dibutuhkan sistem untuk merespons ancaman.

TIN: Terapan Informatika Nusantara
Vol 5, No 7, December 2024, page 414-421
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v5i7.6560

d. Pengurangan Insiden Akses Tidak Sah: Perbandingan jumlah insiden akses tidak sah sebelum dan sesudah penerapan teknologi keamanan.

Tabel 1. perbandingan performa antar metode keamanan

Metrik	Otentikasi Faktor Tunggal	Autentikasi Multi-Faktor	Keamanan Terintegrasi AI
Tingkat Deteksi Ancaman (%)	60	90	95
Tingkat Positif Palsu (%)	15	5	2
Waktu Respons (detik)	10	5	3
Pengurangan Akses Tidak Sah (%)	0	30	35



Gambar 1. Comparison of Security Methods in Digital Libraries

Dari Tabel 1 dan Gambar 1 menunjukkan bahwa perpustakaan digital yang menerapkan autentikasi multifaktor berhasil mengurangi insiden akses tidak sah hingga 30% dibandingkan dengan yang hanya menggunakan autentikasi satu faktor. Selain itu, teknologi enkripsi yang diimplementasikan secara efektif mampu meningkatkan perlindungan terhadap data sensitif, mengurangi risiko kebocoran informasi secara signifikan. Integrasi teknologi AI dalam sistem keamanan perpustakaan digital juga terbukti meningkatkan kemampuan deteksi ancaman secara proaktif, yang memperkuat perlindungan data pengguna.

Jika dibandingkan dengan penelitian sebelumnya, seperti yang dilakukan oleh Liu et al. (2022), yang hanya berfokus pada implementasi enkripsi, penelitian ini memperluas cakupan dengan mengintegrasikan teknologi AI untuk deteksi ancaman proaktif dan autentikasi multifaktor. Selain itu, penelitian oleh Khan et al. (2024) lebih terfokus pada kebijakan keamanan data, sementara penelitian ini menggabungkan kebijakan dengan teknologi secara praktis. Perpustakaan yang mengikuti pendekatan ini menunjukkan peningkatan signifikan dalam kemampuan deteksi ancaman dibandingkan dengan pendekatan sebelumnya yang lebih sederhana.

Dengan memanfaatkan kombinasi teknologi canggih dan kebijakan privasi yang relevan, perpustakaan digital dapat mengatasi tantangan keamanan yang kompleks di era digital ini. Selanjutnya, penggunaan teknologi enkripsi dan pengaturan akses yang ketat merupakan langkah penting dalam mencegah akses yang tidak sah dan menjaga kerahasiaan data pengguna. Enkripsi data memastikan bahwa informasi sensitif diacak sehingga hanya pihak yang berwenang yang dapat membaca dan mengaksesnya. Pengaturan akses yang ketat memastikan bahwa hanya pengguna yang sah yang memiliki akses ke data yang relevan.

Selain itu, implementasi sistem autentikasi multifaktor juga sangat penting. Dengan menggabungkan beberapa faktor otentikasi seperti kata sandi, token, atau sidik jari, sistem ini memperkuat lapisan keamanan dan mengurangi risiko penipuan atau akses tidak sah.

Dari segi hukum, kepatuhan terhadap peraturan privasi seperti GDPR di Uni Eropa sangat penting. Perpustakaan harus memastikan bahwa praktik mereka sejalan dengan regulasi yang berlaku untuk melindungi data pengguna dari penyalahgunaan atau penggunaan yang tidak sah.

Selain itu, edukasi tentang praktik terbaik keamanan siber bagi staf perpustakaan dan pengguna juga krusial. Kesadaran akan ancaman seperti rekayasa sosial dan phishing dapat mengurangi risiko serangan siber yang berhasil. Peningkatan pemahaman tentang potensi risiko dan langkah-langkah pencegahan dapat membantu mengurangi kelemahan dalam sistem keamanan.

Terakhir, pemanfaatan teknologi seperti kecerdasan buatan (AI) dan algoritma pembelajaran mesin dapat membantu dalam mendeteksi dan mencegah ancaman keamanan. Analisis data besar memungkinkan identifikasi pola perilaku yang tidak biasa dan memberikan respons cepat terhadap insiden keamanan yang terjadi.

Dengan menerapkan serangkaian strategi ini, perpustakaan dapat memperkuat perlindungan privasi dan keamanan data pengguna mereka, membangun kepercayaan yang kuat di antara pengguna, dan memastikan kepatuhan

TIN: Terapan Informatika Nusantara
Vol 5, No 7, December 2024, page 414-421
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v5i7.6560

terhadap regulasi yang berlaku.

Hasil penelitian menunjukkan bahwa perpustakaan digital menghadapi tantangan signifikan dalam melindungi privasi dan keamanan data pengguna. Implementasi standar internasional dan teknologi enkripsi yang canggih dapat membantu mengatasi beberapa tantangan ini. Namun, hanya teknologi saja tidak cukup. Perpustakaan juga perlu memastikan kepatuhan terhadap peraturan privasi yang berlaku dan mengedukasi pengguna serta staf tentang pentingnya keamanan data.

privasi yang jelas dan transparan serta memastikan bahwa semua staf memahami dan mematuhi kebijakan tersebut. Selain itu, perpustakaan juga harus mempertimbangkan pertimbangan etis dalam pengelolaan data, termasuk penggunaan algoritma yang etis dan penghormatan terhadap hak kekayaan intelektual.

Edukasi berkelanjutan bagi staf perpustakaan dan pengguna adalah kunci untuk memastikan bahwa mereka sadar akan ancaman keamanan dan privasi. Program pelatihan reguler dan kampanye kesadaran dapat membantu mengurangi risiko serangan siber dan meningkatkan kepatuhan terhadap praktik keamanan terbaik. Pemanfaatan teknologi baru seperti AI dan pembelajaran mesin dapat meningkatkan kemampuan perpustakaan untuk mendeteksi dan merespons ancaman. Teknologi ini memungkinkan deteksi dini perilaku mencurigakan dan respon otomatis yang lebih cepat, sehingga mengurangi dampak potensial dari insiden keamanan.

Secara keseluruhan, perpustakaan digital perlu mengadopsi pendekatan yang komprehensif untuk melindungi privasi dan keamanan data. Ini termasuk implementasi teknologi canggih, kepatuhan terhadap regulasi, dan edukasi berkelanjutan bagi semua pihak yang terlibat. Hanya dengan pendekatan terpadu ini, perpustakaan dapat memastikan keamanan dan integritas sumber daya digital mereka di era digital yang terus berkembang.

4. KESIMPULAN

Penelitian ini menegaskan pentingnya integrasi teknologi keamanan canggih, seperti AI dan autentikasi multifaktor, dengan kebijakan privasi untuk meningkatkan keamanan perpustakaan digital. Temuan utama menunjukkan bahwa teknologi ini secara signifikan meningkatkan deteksi ancaman, mengurangi insiden akses tidak sah, dan memperkuat perlindungan data sensitif. Rekomendasi penelitian mencakup perlunya investasi lebih besar pada teknologi keamanan berbasis AI, pelatihan staf perpustakaan untuk memahami dan mengelola teknologi ini, serta pembaruan regulasi yang relevan dengan perkembangan teknologi. Namun, penelitian ini memiliki keterbatasan pada cakupan geografis yang terbatas dan ketergantungan pada data simulasi, sehingga diperlukan penelitian lebih lanjut dengan studi kasus nyata untuk memvalidasi temuan dan memperluas aplikasinya di berbagai konteks.

REFERENCES

Aldaej, A. (2021). Notice of Retraction: Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI). In *IEEE Access* (p. 1). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/ACCESS.2019.2893445

Alwahedi, F., Aldhaheri, A., Ferrag, M. A., Battah, A., & Tihanyi, N. (2024). Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. In *Internet of Things and Cyber-Physical Systems* (Vol. 4, pp. 167–185). Elsevier BV. https://doi.org/10.1016/j.iotcps.2023.12.003

Biswas, S., & Palamidessi, C. (2024). PRIVIC: A privacy-preserving method for incremental collection of location data. In *Proceedings on Privacy Enhancing Technologies* (Vol. 2024, Issue 1, pp. 582–596). Privacy Enhancing Technologies Symposium Advisory Board. https://doi.org/10.56553/popets-2024-0033

Brighente, A., Conti, M., Renzone, G. Di, Peruzzi, G., & Pozzebon, A. (2024). Security and Privacy of Smart Waste Management Systems: A Cyber-Physical System Perspective. In *IEEE Internet of Things Journal* (Vol. 11, Issue 5, pp. 7309–7324). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/JIOT.2023.3322532

Chen, H., & Babar, M. A. (2024). Security for Machine Learning-based Software Systems: A Survey of Threats, Practices, and Challenges. In *ACM Computing Surveys* (Vol. 56, Issue 6, pp. 1–38). Association for Computing Machinery (ACM). https://doi.org/10.1145/3638531

Davies, J. (2023). Enhanced scalability and privacy for blockchain data using Merklized transactions. In *Frontiers in Blockchain* (Vol. 6). Frontiers Media SA. https://doi.org/10.3389/fbloc.2023.1222614

Demirer, M., Jiménez Hernández, D., Li, D., & Peng, S. (2024). Data, Privacy Laws and Firm Production: Evidence from the GDPR. In *SSRN Electronic Journal*. Elsevier BV. https://doi.org/10.2139/ssrn.4718871

Du, Z., Li, Y., Fu, Y., & Zheng, X. (2024). Blockchain-based access control architecture for multi-domain environments. In *Pervasive and Mobile Computing* (Vol. 98, p. 101878). Elsevier BV. https://doi.org/10.1016/j.pmcj.2024.101878

Eghmazi, A., Ataei, M., Landry, R. J., & Chevrette, G. (2024). Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy. In *Internet of Things* (Vol. 5, Issue 1, pp. 20–34). MDPI AG. https://doi.org/10.3390/iot5010002

Filani, J. (2024). Data Privacy in the Digital Age: Analyzing the impact of Technology of U.S Privacy Regulations. In *SSRN Electronic Journal*. Elsevier BV. https://doi.org/10.2139/ssrn.4762809

Hanisch, S., Todt, J., Patino, J., Evans, N., & Strufe, T. (2024). A False Sense of Privacy: Towards a Reliable

Evaluation Methodology for the Anonymization of Biometric Data. In *Proceedings on Privacy Enhancing Technologies* (Vol. 2024, Issue 1, pp. 116–132). Privacy Enhancing Technologies Symposium Advisory Board. https://doi.org/10.56553/popets-2024-0008

Hashem, T. N. (2024). Examining marketing cyber-security in the digital age: Evidence from marketing platforms. In *International Journal of Data and Network Science* (Vol. 8, Issue 2, pp. 1141–1150). Growing Science. https://doi.org/10.5267/j.ijdns.2023.11.020

Khan, I. A., Razzak, I., Pi, D., Khan, N., Hussain, Y., Li, B., & Kousar, T. (2024). Fed-Inforce-Fusion: A federated reinforcement-based fusion model for security and privacy protection of IoMT networks against cyber-attacks. In *Information Fusion* (Vol. 101, p. 102002). Elsevier BV. https://doi.org/10.1016/j.inffus.2023.102002

Kumari, P., Natesan, D. G., & Kumar, M. (2024). Exploring Frontiers in Big Data: Privacy-Preserving Exchange and Data Lake Innovations. In *International Journal of Research Publication and Reviews* (Vol. 5, Issue 3, pp. 862–865). Genesis Global Publication. https://doi.org/10.55248/gengpi.5.0324.0637

Kutschera, S., Slany, W., Ratschiller, P., Gursch, S., Deininger, P., & Dagenborg, H. (2024). Incidental Data: A Survey towards Awareness on Privacy-Compromising Data Incidentally Shared on Social Media. In *Journal of Cybersecurity and Privacy* (Vol. 4, Issue 1, pp. 105–125). MDPI AG. https://doi.org/10.3390/jcp4010006

Ling, J., Zheng, J., & Chen, J. (2024). Efficient federated learning privacy preservation method with heterogeneous differential privacy. In *Computers and Security* (Vol. 139, p. 103715). Elsevier BV. https://doi.org/10.1016/j.cose.2024.103715

Liu, J., Tang, Y., Zhao, H., Wang, X., Li, F., & Zhang, J. (2024). CPS Attack Detection under Limited Local Information in Cyber Security: An Ensemble Multi-Node Multi-Class Classification Approach. In *ACM Transactions on Sensor Networks* (Vol. 20, Issue 2, pp. 1–27). Association for Computing Machinery (ACM). https://doi.org/10.1145/3585520

Liu, Z., Guo, J., Yang, W., Fan, J., Lam, K. Y., & Zhao, J. (2022). Privacy-Preserving Aggregation in Federated Learning: A Survey. In *IEEE Transactions on Big Data* (pp. 1–20). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/TBDATA.2022.3190835

Manalo, M. L. B., & Gallardo, R. D. (2024). Cyber Security Awareness and Educational Outcomes of Grade 4 Learners. In *International Journal of Innovative Science and Research Technology (IJISRT)* (pp. 1390–1422). International Journal of Innovative Science and Research Technology. https://doi.org/10.38124/ijisrt/ijisrt24apr1261

Masood, I., Daud, A., Wang, Y., Banjar, A., & Alharbey, R. (2024). A blockchain-based system for patient data privacy and security. In *Multimedia Tools and Applications*. Springer Science and Business Media LLC. https://doi.org/10.1007/s11042-023-17941-y

Mlika, F., Karoui, W., & Romdhane, L. Ben. (2024). Blockchain solutions for trustworthy decentralization in social networks. In *Computer Networks* (Vol. 244, p. 110336). Elsevier BV. https://doi.org/10.1016/j.comnet.2024.110336

Munilla Garrido, G., Nair, V., & Song, D. (2024). SoK: Data Privacy in Virtual Reality. In *Proceedings on Privacy Enhancing Technologies* (Vol. 2024, Issue 1, pp. 21–40). Privacy Enhancing Technologies Symposium Advisory Board. https://doi.org/10.56553/popets-2024-0003

Patil, R. A., & Patil, P. D. (2024). Efficient approximation and privacy preservation algorithms for real time online evolving data streams. In *World Wide Web* (Vol. 27, Issue 1). Springer Science and Business Media LLC. https://doi.org/10.1007/s11280-024-01244-9

Sedlak, B., Murturi, I., Donta, P. K., & Dustdar, S. (2023). A Privacy Enforcing Framework for Data Streams on the Edge. In *IEEE Transactions on Emerging Topics in Computing* (pp. 1–12). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/TETC.2023.3315131

Seeman, J., & Susser, D. (2024). Between Privacy and Utility: On Differential Privacy in Theory and Practice. In *ACM Journal on Responsible Computing* (Vol. 1, Issue 1, pp. 1–18). Association for Computing Machinery (ACM). https://doi.org/10.1145/3626494

Sharma, S., & Dwivedi, R. (2024). A survey on blockchain deployment for biometric systems. In *IET Blockchain*. Institution of Engineering and Technology (IET). https://doi.org/10.1049/blc2.12063

Sharma, S., & Nebhnani, M. (2024). Securing the Digital Frontier: Data Science Applications in Cyber security and Anomaly Detection. In *International Journal of Food and Nutritional Sciences* (Vol. 09, Issue 03). Institute for Advanced Studies. https://doi.org/10.48047/ijfans/09/03/33

Singh, R. K. (2024). Developing a big data analytics platform using Apache Hadoop Ecosystem for delivering big data services in libraries. In *Digital Library Perspectives* (Vol. 40, Issue 2, pp. 160–186). Emerald. https://doi.org/10.1108/DLP-10-2022-0079

Song, F., Li, L., Yikun, Li, Ma, Y., Wang, L., & Zhang, H. (2021). Smart Collaborative Contract for Endogenous Access Control in Massive Machine Communications. In *IEEE Internet of Things Journal* (p. 1). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/JIOT.2021.3134366

Subramani, J., Maria, A., Rajasekaran, A. S., & Lloret, J. (2024). Physically secure and privacy-preserving blockchain enabled authentication scheme for internet of drones. In *Security and Privacy* (Vol. 7, Issue 3). Wiley. https://doi.org/10.1002/spy2.364

Tosi, D., Kokaj, R., & Roccetti, M. (2024). 15 years of Big Data: a systematic literature review. In *Journal of Big Data*


TIN: Terapan Informatika Nusantara
Vol 5, No 7, December 2024, page 414-421
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v5i7.6560

(Vol. 11, Issue 1). Springer Science and Business Media LLC. https://doi.org/10.1186/s40537-024-00914-9

Wen, X., Chen, Y., Zhang, W., Jiang, Z. L., & Fang, J. (2024). Quantum protection scheme for privacy data based on trusted center. In *Optics and Laser Technology* (Vol. 169, p. 110130). Elsevier BV. https://doi.org/10.1016/j.optlastec.2023.110130

Wu, C. (2024). Data privacy: From transparency to fairness. In *Technology in Society* (Vol. 76, p. 102457). Elsevier BV. https://doi.org/10.1016/j.techsoc.2024.102457

Zhang, K., Chen, K., Li, Z., Chen, J., & Zheng, Y. (2023). Privacy-Preserving Data-Enabled Predictive Leading Cruise Control in Mixed Traffic. In *IEEE Transactions on Intelligent Transportation Systems* (pp. 1–16). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/TITS.2023.3329484