DOI: 10.37014/medpus.v31i3.5317

media pustakawan

Keamanan Informasi dan Privasi Pengguna dalam Layanan Perpustakaan Digital

Cindy Amelia Putri[1*], Rully Khairul Anwar[2], Siti Chaerani Djen Amar[3], Evi Nursanti Rukmana[4]

[1,2,3,4] Universitas Padjadjaran, Sumedang, Indonesia
Jln. Ir. Soekarno km. 21 Jatinangor, Kab. Sumedang 45363 Jawa Barat

*Korespondensi: *cindy23004@mail.unpad.ac.id*

Diajukan: 09-09-2024; **Direvisi:** 16-12-2024; **Diterima:** 18-12-2024

Abstract

The development of libraries from conventional to digital-based libraries has brought significant impacts on the way library services are provided and accessed by users. However, along with its benefits, digital libraries face new challenges related to data security and user privacy such as effective protection of personal data. This research aims to analyze security and privacy threats in digital library services and identify the implementation of security technologies and privacy policies in this context. This research uses the narrative literature review method to analyze 12 references relevant to the topic of information security and user privacy in digital library services. This research has security and privacy risks involved in digital library services, how security technologies are implemented, and how privacy regulations and policies impact the situation. Results show that virus attacks and brute force attacks are some of the security threats of digital libraries. To protect sensitive user data, the use of security technologies such as data encryption and the use of firewalls are also very important. Privacy regulations and policies such as GDPR go a long way in helping digital libraries maintain the privacy of their users. This analysis enhances our understanding of the problems and solutions in data security management and user privacy in digital library services. Thus, this research highlights the importance of managing information security and user privacy in the context of digital library services to ensure optimal protection of sensitive user data.

Keywords: information security; user privacy; digital library

Abstrak

Perkembangan perpustakaan dari sistem konvensional menuju perpustakaan berbasis digital telah memberikan dampak besar pada cara perpustakaan dalam menyediakan layanan dan bagaimana pengguna dapat mengakses informasi tersebut. Namun, bersamaan dengan manfaatnya, perpustakaan digital menghadapi tantangan baru terkait keamanan data dan privasi pengguna seperti perlindungan yang efektif terhadap data pribadi. Penelitian ini bertujuan untuk menganalisis ancaman keamanan dan privasi dalam layanan perpustakaan digital serta mengidentifikasi implementasi teknologi keamanan dan kebijakan privasi dalam konteks ini. Penelitian ini menggunakan metode *narrative literature review* untuk menganalisis 12 referensi yang relevan dengan topik keamanan informasi dan privasi pengguna dalam layanan perpustakaan digital. Penelitian ini memiliki risiko keamanan dan privasi yang terlibat dalam layanan perpustakaan digital, bagaimana teknologi keamanan diterapkan, dan bagaimana peraturan dan kebijakan privasi berdampak pada situasi tersebut. Hasil menunjukkan bahwa serangan virus dan serangan *brute force* adalah beberapa ancaman keamanan perpustakaan digital. Untuk melindungi data pengguna yang sensitif, penggunaan teknologi keamanan seperti enkripsi data dan penggunaan *firewall* juga sangat penting. Peraturan dan kebijakan privasi seperti GDPR sangat membantu perpustakaan digital menjaga privasi penggunanya. Analisis ini meningkatkan pemahaman kita tentang masalah dan solusi dalam manajemen keamanan data dan privasi pengguna dalam layanan perpustakaan digital. Dengan demikian, penelitian ini menyoroti pentingnya pengelolaan keamanan informasi dan privasi pengguna dalam konteks layanan perpustakaan digital untuk memastikan perlindungan yang optimal terhadap data sensitif pengguna.

Kata Kunci: keamanan informasi; privasi pengguna; perpustakaan digital

Pendahuluan

Selama beberapa dekade terakhir ini, perkembangan teknologi informasi dan komunikasi telah memengaruhi sistem layanan perpustakaan. Pada awalnya, layanan perpustakaan dilakukan secara konvensional dengan cara mengunjungi perpustakaan secara langsung ke tempat perpustakaan itu berada. Namun dewasa ini, terjadi pergeseran layanan perpustakaan ke arah modern yang menyediakan perpustakaan berbasis digital. Perpustakaan berbasis digital ini memanfaatkan teknologi informasi untuk menyimpan koleksi-koleksi dalam format digital yang dapat diakses secara fleksibel dan praktis, tidak terbatas waktu dan lokasi, serta distribusi informasi terjadi dengan cepat, tepat, dan akurat (Widayanti, 2015).

Layanan perpustakaan digital ini memungkinkan pengguna untuk dapat mengakses koleksi buku dan informasi lainnya secara *online* tanpa harus secara fisik datang ke perpustakaan. Perpustakaan digital memberikan akses kepada pengguna untuk menikmati beragam layanan, seperti penelusuran dan peminjaman buku secara daring, diskusi kelompok virtual dan berbagi sumber daya pengetahuan melalui platform daring. Dengan demikian, perpustakaan digital tidak hanya memberikan akses untuk koleksi data tetapi juga menciptakan ruang interaktif yang nantinya dapat membuat pengguna lebih mudah mengakses dan menggunakan informasi. Dengan demikian, perpustakaan digital adalah sarana yang efektif untuk membantu masyarakat secara luas meningkatkan literasi informasi dan pembelajaran sepanjang hayat.

Salah satu aspek penting yang harus dipertimbangkan dalam pengembangan layanan perpustakaan digital adalah keamanan informasi dan privasi pengguna. Transformasi digital perpustakaan menciptakan ancaman baru dalam bidang *cyber security*. Perpustakaan digital tentunya harus memastikan bahwa sistem yang digunakan dilengkapi dengan perlindungan terhadap *cyber attack*. *Cyber attack* merupakan tindakan kejahatan yang dilakukan oleh seseorang dengan tujuan merusak jaringan atau sistem komputer. Contoh ancaman dalam konteks perpustakaan digital, seperti *malware* dapat menyebabkan terjadinya ancaman keamanan informasi dan privasi pengguna. *Malware* merupakan perangkat lunak berbahaya yang dapat merusak sistem dan mencuri data. Berbagai jenis *malware*, seperti virus, *ransomware*, dan *trojan horse*, dapat mengancam integritas data dalam perpustakaan digital. Sebagai contoh pada jurnal Setiano et al. (2024), *ransomware* dapat mengenkripsi data dan meminta tebusan untuk mengembalikannya. Kasus nyata terjadi pada Perpustakaan Umum St. Louis di Amerika Serikat yang diserang pada tahun 2017, di mana *hacker* meminta Bitcoin untuk membuka akses ke server yang diretas. Penelitian menunjukkan bahwa risiko keselamatan data perpustakaan digital tidak hanya berasal dari aplikasi yang digunakan tetapi juga dari objek fisik yang menyimpan data.

Penelitian mengenai layanan perpustakaan berbasis digital telah banyak dilakukan oleh peneliti lain. Dalam artikel ini, penulis memilih dua penelitian terdahulu yang relevan untuk dibandingkan yaitu penelitian oleh Triandari (2022) dan Galih (2020). Pemilihan kedua penelitian ini didasarkan pada kesesuaian fokus kajian mereka terhadap aspek keamanan informasi dan privasi pengguna dalam layanan perpustakaan digital, yang menjadi inti dari penelitiaan ini. Penelitian Triandari (2022) membahas tentang sistem keamanan informasi pada perpustakaan digital (*security and privacy system*) secara lebih mendalam, ancaman keamanan informasi pada perpustakaan digital, serta pencegahan ancaman keamanan informasi yang dapat dilakukan oleh pustakawan. Sementara itu, penelitian Galih (2020) menitikberatkan pada keamanan informasi aplikasi iPusnas, dengan temuan utama dari penelitian tersebut adalah bahwa aplikasi iPusnas telah memperhatikan dan mengimplementasikan langkah-langkah keamanan informasi, seperti kebijakan lisensi, prosedur pendaftaran anggota yang memerlukan verifikasi, serta penggunaan teknologi keamanan seperti *Secure Socket Layer* (SSL) untuk melindungi transmisi data pengguna.

Kedua penelitian terdahulu tersebut memiliki kesamaan fokus dalam aspek keamanan informasi dan privasi pengguna dalam layanan perpustakaan digital. Perbedaan utama penelitian

penulis dengan penelitian terdahulu terletak pada fokus dan pendekatan yang digunakan dalam menghadapi tantangan keamanan informasi dan privasi pengguna dalam layanan perpustakaan digital. Kedua penelitian terdahulu tersebut hanya membahas salah satu dari aspek keamanan informasi atau privasi pengguna, sedangkan penelitian ini membahas kedua aspek tersebut. Meskipun penelitian terdahulu telah menggarisbawahi pentingnya manajemen keamanan informasi dan privasi, serta implementasi teknologi keamanan dalam konteks perpustakaan digital, dalam penelitian ini penulis menekankan beberapa aspek. Mengacu pada hal tersebut, pertanyaan yang diajukan dalam penelitian ini adalah (1) Apa saja ancaman keamanan yang paling sering dihadapi oleh layanan perpustakaan digital saat ini? (2) Bagaimana implementasi teknologi keamanan dapat membantu melindungi informasi sensitif pengguna dalam perpustakaan digital? (3) Bagaimana regulasi dan kebijakan privasi memengaruhi praktik keamanan informasi dalam layanan perpustakaan digital? Tujuan penelitian ini adalah (1) Mengetahui ancaman keamanan yang paling sering dihadapi oleh layanan perpustakaan digital saat ini, (2) Memahami implementasi teknologi keamanan dan kaitannya dalam membantu melindungi informasi sensitif pengguna dalam perpustakaan digital, (3) Memahami regulasi dan kebijakan privasi dalam memengaruhi praktik keamanan informasi dalam layanan perpustakaan digital.

Tinjauan Pustaka

Menurut Farid et al. (2023), keamanan informasi didefinisikan sebagai serangkaian proses yang bertujuan untuk melindungi informasi dan sumber daya data dari ancaman berbagai resiko. Konsep ini tidak hanya menekankan perlindungan data terhadap privasi, keakuratan, dan ketersediaan data, serta mencegah akses penggunaan atau perubahan informasi secara tidak sah. Keamanan informasi ini melibatkan berbagai aspek, mulai dari penerapan *hight tech* hingga penggunaan data yang tidak sah. Keamanan informasi juga membutuhkan kerja sama dari berbagai disiplin ilmu dan departemen dalam organisasi, bukan hanya satu tindakan atau teknologi. Ini memerlukan pemahaman mendalam tentang berbagai anacaman keamanan. Keamanan informasi adalah komponen penting dari sistem, bukan hanya bergantung teknologi atau prosedur. Ini mencakup berbagai tindakan yang dimaksudkan untuk melindungi data dan sistem dari ancaman dan bahaya yang mungkin terjadi.

Keamanan informasi berkaitan dengan proses, bukan prosedur atau teknologi dengan karakteristik yang meliputi kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) (Alkhudhayr et al., 2019). Samonas & Coss (2014) menjelaskan lebih lanjut konsep mengenai kerahasiaan, integritas, dan ketersediaan sebagai berikut:

1. Kerahasiaan (*confidentiality*), menekankan perlindungan data dan informasi dari akses atau pengungkapan yang tidak sah dan merupakan prinsip utama dalam aspek keamanan infromasi.
2. Integritas (*integrity*), integritas menjamin bahwa informasi tetap utuh, benar, dan tidak diubah secara tidak sah. Integritas melibatkan pemeliharaan ketepatan dan kelengkapan data serta mencegah modifikasi atau penghancuran data. Integritas juga mencakup perilaku etis, tanggung jawab, dan kepatuhan terhadap standar profesional serta konsep-konsep seperti keaslian dan non-repudiasi, memastikan bahwa data asli dan transaksi tidak dapat disangkal.
3. Ketersediaan (*availability*), menekankan pentingnya akses yang tepat waktu dan andal terhadap informasi. Hal ini berarti memastikan bahwa informasi dapat diakses ketika diperlukan dan tidak terhalang oleh gangguan atau hambatan.

Seperti yang dijelaskan oleh Samonas & Coss (2014), konsep tersebut menawarkan dasar yang kuat untuk memahami dasar keamanan informasi. Profesional teknologi informasi yang memahami konsep ini dapat merancang sistem keamanan yang efisien serta menerapkan strategi yang lebih canggih dan fleksibel untuk menghadapi ancaman *cyber* dan fisik yang terus berkembang. Konsep tersebut tidak hanya efisien tetapi juga responsif terhadap tantangan yang terus muncul dalam

dunia digital modern. Penggunaan prinsip keamanan ini, saat mengembangkan perpustakaan digital akan memastikan bahwa data yang disimpan dan diakses oleh pengguna tetap aman, utuh, dan tersedia dengan tepat waktu. Selain itu, penerapan prinsip-prinsip ini akan meningkatkan kepercayaan masyarakat terhadap perpustakaan digital.

Privasi pengguna mencakup hak setiap orang untuk mengontrol informasi pribadi mereka. Ini mencakup tidak hanya bagaimana data dikumpulkan, disimpan, digunakan, dan dibagikan dengan orang lain, tetapi juga cara data dilindungi dan dikelola di dunia digital (Hess et al., 2015). Perlindungan privasi pengguna dalam layanan perpustakaan digital yang semakin berkembang menjadi semakin sulit dan mendesak. Ini terutama berlaku untuk perlindungan data sensitif seperti riwayat peminjaman, preferensi bacaan, dan informasi identitas. Di samping itu, upaya tersebut juga harus mempertimbangkan ancaman dari pihak yang tidak sah atau penyalahgunaan data oleh entitas yang tidak berwenang. Hal ini dapat mengancam keamanan dan integritas data pengguna secara keseluruhan. Oleh karena itu, penerapan kebijakan dan mekanisme perlindungan privasi yang efektif sangat penting untuk menumbuhkan kepercayaan pengguna terhadap layanan perpustakaan digital dan memastikan bahwa hak privasi individu tetap dilindungi di era internet.

Sun et al. (2014) menjelaskan permasalahan terkait privasi dapat dikategorikan menjadi empat, yakni:

1. Kontrol data pengguna, mengacu pada cara untuk memberikan pengguna kontrol atas data mereka saat disimpan dan diproses, serta mencegah pencurian, kejahatan, dan penjualan tidak sah.
2. Replikasi data mengacu pada cara memastikan replikasi data pengguna di berbagai lokasi sesuai yurisdiksi dengan menjaga konsistensi data, mencegah kehilangan dan kebocoran data, serta perubahan atau penyisipan data palsu yang tidak sah.
3. Tanggung jawab hukum, menentukan pihak yang bertanggung jawab untuk memenuhi persyaratan hukum terkait informasi pribadi yang disimpan dan diproses.
4. Peran subkontraktor, mengacu pada sejauh mana subkontraktor terlibat dalam pemrosesan data yang dapat diidentifikasi, diperiksa, dan dipastikan dengan benar, serta bagaimana mengelola keterlibatan mereka untuk menjaga privasi pengguna.

Penjelasan tersebut sangat berguna untuk memahami kompleksitas masalah privasi yang terkait dengan teknologi informasi kontemporer. Penerapan kebijakan dan prosedur perlindungan privasi yang kuat sangat penting untuk menumbuhkan kepercayaan pengguna terhadap layanan perpustakaan digital. Langkah-langkah ini tidak hanya diperlukan untuk menjaga keamanan data pengguna, tetapi juga untuk menjamin hak privasi individu tetap aman di tengah gejolak era internet yang penuh dengan tantangan. Oleh karena itu, memahami secara menyeluruh tentang kompleksitas masalah privasi yang terkait dengan teknologi informasi kontemporer sangat penting untuk mengembangkan pendekatan yang holistik dan berbasis bukti untuk menyelesaikan masalah ini.

Perpustakaan merupakan tempat yang dibutuhkan oleh masyarakat sebagai sumber untuk mendapatkan informasi. Melalui perpustakaan masyarakat bisa mendapatkan kebutuhan sumber daya infomasi, baik itu berupa cetak ataupun non-cetak. Dengan demikian, perpustakaan memiliki peran yang sangat penting dalam memberikan akses dan mendukung pengembangan pengetahuan serta literasi masyarakat secara luas. Seiring perkembangan zaman, tentu perpustakaan akan berkembang, salah satunya perpustakaan digital. Perpustakaan digital merupakan perpustakaan hasil dari inovasi pengembangan perpustakaan. Perpustakaan digital dirancang untuk menarik lebih banyak pengguna dari berbagai lapisan masyarakat, sekaligus memperluas jangkauan layanan ke kelompok-kelompok baru yang sebelumnya sulit dijangkau. Mengembangkan perpustakaan digital adalah salah satu cara

terbaik untuk mengoptimalkan penggunaan media distribusi informasi secara merata. Meskipun perpustakaan digital bukanlah faktor utama dalam mendorong masyarakat untuk menggunakan perpustakaan, keberadaannya cukup signifikan sebagai alat penting untuk berkomunikasi dan menyebarkan informasi.

Menurut Triandari (2022), perpustakaan digital adalah lembaga yang mengumpulkan dan mengelola koleksi data dalam bentuk digital melalui penggunaan sistem otomatisasi. Perpustakaan digital bertujuan untuk memberikan akses cepat dan efisien kepada masyarakat terhadap informasi yang mereka butuhkan. Ini dapat dicapai dengan menggunakan teknologi yang memungkinkan penyimpanan dan pengorganisasian data secara virtual, tanpa memerlukan ruang fisik untuk menyimpan koleksi data. Perpustakaan digital harus terus berubah dan berkembang untuk memenuhi kebutuhan masyarakat akan informasi. Ini termasuk memanfaatkan teknologi baru seperti AI (*artificial intelligence*) dan analisis data untuk meningkatkan relevansi dan aksesibilitas informasi yang mereka tawarkan.

Menurut Wahda (2020), perpustakaan digital merupakan suatu entitas yang terorganisasi secara sistematis, terdiri dari infrastruktur teknologi seperti perangkat keras dan perangkat lunak yang dirancang khusus, serta koleksi elektronik yang mencakup beragam materi sumber daya informasi digital seperti *e-book*, jurnal elektronik, basis data, dan lain sebagainya. Di samping itu, perpustakaan digital juga melibatkan peran staf profesional yang bertanggung jawab dalam proses pengelolaan, pengelompokan, dan pemeliharaan koleksi digital tersebut. Perpustakaan digital memfasilitasi distribusi dan akses informasi secara cepat dan luas, melampaui batasan geografis dan waktu yang mungkin ada dalam perpustakaan konvensional. Perpustakaan digital memungkinkan pengguna mengakses koleksi digital dari mana saja dan kapan saja melalui koneksi internet. Selain berfungsi sebagai tempat penyimpanan dan akses informasi, perpustakaan digital juga berperan sebagai pusat interaksi dan pertukaran intelektual dalam era digital yang terus berkembang. Sebagai sistem informasi yang terhubung secara *online*, perpustakaan digital memudahkan pengguna dalam memperoleh informasi, baik untuk kebutuhan pembelajaran, penelitian, maupun hiburan.

Metodologi Penelitian

Pada Penelitian ini penulis menggunakan metode *narrative literature review* untuk menganalisis beragam literatur yang relevan dengan topik keamanan informasi dan privasi pengguna dalam layanan perpustakaan digital. Penelitian *literatur review* sendiri adalah metode penelitian yang bertujuan untuk mengeksplorasi, menggambarkan, dan menganalisis berbagai konsep, hasil, dan metode yang ada dalam literatur yang relevan. Selain itu, *literatur review* adalah sebuah karya tulis yang bertujuan untuk menyajikan argumen-argumen yang didasarkan pada pemahaman mendalam tentang keadaan pengetahuan saat ini tentang suatu topik tertentu. Dengan menggunakan tinjauan literatur, penulis memiliki kesempatan untuk membangun sebuah rangkaian argumen yang meyakinkan dengan tujuan untuk memberikan jawaban yang meyakinkan terhadap pertanyaan penelitian. Seperti yang dijelaskan oleh Machi & McEvoy (2022), peninjauan literatur tidak hanya mengumpulkan informasi, tetapi juga melibatkan proses analisis dan sintesis yang cermat terhadap literatur yang relevan. Proses dalam melakukan *literatur review* melibatkan penentuan topik, mengembangkan alat argumentasi, mencari literatur, survei literatur, kritik literatur, dan menulis *review*. *Narrative literature review* dipilih karena memungkinkan penulis untuk menyajikan ringkasan yang komprehensif terkait penelitian terdahulu yang relevan dengan topik penelitian ini. Pendekatan ini juga memungkinkan untuk mendokumentasikan, menganalisis, dan menyimpulkan tentang apa yang diketahui terkait topik keamanan informasi dan privasi pengguna dalam layanan perpustakaan digital. Data yang dikumpulkan untuk penelitian ini dikumpulkan dari bulan Maret

hingga April 2024. Saat ini, penulis melakukan pencarian, seleksi, dan analisis literatur tentang keamanan data dan privasi pengguna dalam layanan perpustakaan digital. Literatur yang dikumpulkan mencakup penelitian terbaru yang mendukung tujuan penelitian dan memberikan gambaran lengkap tentang kemajuan dalam bidang ini. Oleh karena itu, saya ingin memastikan bahwa literatur yang diulas mencerminkan pengetahuan saat ini tentang topik penelitian.

Untuk mendapatkan data penelitian yang relevan, peneliti menggunakan *database* akademik Google Scholar untuk melakukan pencarian literatur. Kata kunci yang dianggap relevan digunakan untuk melakukan pencarian dalam bahasa Indonesia, seperti "keamanan informasi", "privasi pengguna", dan "layanan perpustakaan digital", serta dalam bahasa Inggris, seperti "*information security*", "*user privacy*", dan "*digital library*". Tujuan dari langkah ini adalah untuk memastikan bahwa rentang penelusuran mencakup semua literatur yang mungkin relevan dengan topik penelitian. Pencarian dilakukan dengan memperhatikan rentang waktu dari tahun 2014 hingga 2024 untuk memastikan inklusi literatur terbaru yang dapat memberikan pemahaman yang komprehensif tentang topik yang diteliti. Setelah mengumpulkan hasil penelitian, peneliti menyortir dan memilih literatur berdasarkan sejumlah kriteria, termasuk relevansi dengan topik penelitian, kualitas sumber, dan signifikansi hasil dari setiap referensi. Proses penyortiran dilakukan dengan hati-hati untuk memastikan bahwa hanya literatur yang relevan dan berkualitas tinggi yang dipertimbangkan untuk analisis selanjutnya. Oleh karena itu, proses pengumpulan data melalui pencarian literatur Google Scholar mencakup penggunaan kata kunci yang tepat, pemilihan rentang waktu yang sesuai, dan penyortiran hasil berdasarkan kriteria relevansi dan kualitas. Proses ini memungkinkan peneliti untuk mengumpulkan data yang representatif dan berkualitas tinggi untuk digunakan dalam penelitian mendatang.

Teknik analisis data dalam penelitian ini mengadopsi pendekatan yang disarankan oleh Machi & McEvoy (2022). Pertama, data yang didapatkan dari literatur dikelompokkan sesuai dengan kriteria yang telah ditetapkan sebelumnya. Kedua, penyajian data yang mencakup pengorganisasian dan penyajian informasi serta membangun argumen. Terakhir, analisis mendalam terhadap pola data. Temuan penelitian dianalisis untuk mengekstrak pola, tren, atau implikasi penting yang berkaitan dengan keamanan informasi dan privasi pengguna dalam layanan perpustakaan digital. Proses ini akan memungkinkan penulis untuk menyusun kesimpulan yang solid dan memverifikasi hasil penelitian dengan cara yang sistematis dan terperinci. Setiap langkah dalam penelitian ini dilakukan secara sistematis dan terstruktur, dengan proses analisis data yang mengikuti pendekatan yang telah direkomendasikan. Dengan demikian, hasil penelitian dapat dipertahankan secara akurat, sehingga kesimpulan yang dibuat dapat diandalkan. Selain itu, penulis dapat menjelaskan penelitian dengan lebih jelas dengan menggunakan metode ini.

Hasil dan Pembahasan

Ancaman Keamanan dan Privasi dalam Layanan Perpustakaan Digital

Transformasi perpustakaan dari model konvensional menjadi perpustakaan berbasis digital memungkinkan akses yang lebih mudah dan luas bagi pengguna. Namun, bersamaan dengan keuntungan ini, muncul berbagai ancaman yang dapat menyerang keamanan informasi dan privasi pengguna. Ancaman terhadap informasi dapat menyebabkan kerusakan atau kerugian dalam berbagai cara, mulai dari informasi kecil hingga kehancuran seluruh sistem (Pandey & Misra, 2014). Kerusakan atau kehilangan seperti ini dapat membahayakan kerahasiaan atau integritas data dan mengurangi kepercayaan terhadap sistem informasi, bahkan dapat membawa dampak yang lebih besar.

Seperti yang disampaikan oleh Liu (2019), perpustakaan digital yang terhubung dengan jaringan eksternal seperti internet berpotensi menjadi target peretasan yang mengancam, seperti pelepasan virus, pencurian akun pengguna secara ilegal, dan penghancuran data sumber daya.

Konsekuensinya dapat sangat merugikan, seperti kemacetan jaringan, kerusakan server, dan kehilangan data pengguna yang berujung pada gangguan layanan informasi yang normal. Menghadapi tantangan ini, keamanan *cyber* menjadi aspek yang tidak bisa diabaikan, memerlukan strategi yang kokoh dan berkelanjutan untuk mencegah dan merespon ancaman-ancaman tersebut secara efektif, demi melindungi integritas dan keamanan informasi perpustakaan digital, serta memastikan kelancaran layanan informasi kepada pengguna.

Studi yang dilakukan oleh Han et al. (2016) menunjukkan bahwa terdapat dua item risiko tingkat tinggi dalam perpustakaan digital yang tercermin secara khusus dalam aset fisik (komputer-server, perangkat keamanan-*fireproof wall hardware*), ancaman serangan kata sandi dan kerentanan perlindungan kata sandi perangkat lunak. Dalam lingkungan digital, kata sandi adalah lapisan pertahanan utama yang melindungi akses ke informasi sensitif. Ancaman terhadap keamanan kata sandi dapat datang dalam bentuk serangan *brute force*, *phishing*, atau bahkan penyerangan jaringan yang bertujuan untuk merusak keamanan perangkat lunak yang digunakan dalam perpustakaan digital. Kerentanan dalam perlindungan kata sandi perangkat lunak dapat memberikan celah bagi pihak yang tidak berwenang untuk mengakses informasi penting atau merusak integritas data.

Studi yang dilakukan oleh Yusuf et al. (2021) juga berhasil mengidentifikasi ancaman yang dapat menyerang keamanan dalam layanan perpustakaan digital yang dikategorikan menjadi ancaman dalam aspek *hardware security*, *software security*, *network security*, *data security*, dan *physical and human threat*. Ancaman *hardware security* dapat meliputi *electromagnetic interference*, kegagalan peralatan komunikasi, *hardware/equipments failure*, *installation/use of unauthorised hardware*, *maintenance errors*, *malware* dan kode berbahaya. Dalam aspek *software security*, beberapa ancaman tersebut adalah *unauthorised changes to software settings*, *password attacks/sniffing/stealing*, dan *adware and spyware*. Sedangkan dalam aspek *network security*, beberapa di antaranya adalah *e-mail attacks/spams/fraud*, *hacking/intrusion/unauthorised access*, dan *distributed denial of service attacks* (DDoS). DDoS dapat mengganggu layanan perpustakaan digital, membuatnya tidak dapat diakses oleh pengguna yang sah dan mengakibatkan kerugian finansial dan reputasi bagi perpustakaan.

Dari studi yang dilakukan oleh Han et al. (2016) dan Yusuf et al. (2021) menunjukan berbagai ancaman keamanan perpustakaan digital. Mulai dari aset fisik, seperti komputer server hingga ancaman dari *software*, *network*, dan bahkan elemen fisik dan manusia, ancaman tersebut mencakup berbagai elemen. Pertama, seperti aset fisik, perpustakaan digital dapat mengalami masalah teknis yang dapat mengganggu layanan. Masalah teknis ini dapat berasal dari masalah peralatan komunikasi, masalah perangkat keras, atau bahkan instalasi perangkat keras yang tidak sah. Selain itu, serangan *malware* dan kode berbahaya merupakan bahaya yang signifikan bagi keamanan perpustakaan digital. Kedua, dalam hal *software*, studi tersebut menunjukkan bahwa perlindungan terhadap kata sandi adalah lapisan pertahanan utama yang diperlukan untuk melindungi akses ke data sensitif. Serangan *brute force*, *phishing*, atau penyerangan jaringan adalah beberapa sumber ancaman keamanan kata sandi. Selain itu, kelemahan dalam perlindungan kata sandi perangkat lunak dapat memungkinkan orang yang tidak berwenang mengakses data sensitif atau merusak integritas data. Ketiga, dalam hal jaringan, perpustakaan digital menghadapi ancaman seperti serangan *e-mail*, *hacking*, dan serangan DDoS. Serangan DDoS terutama dapat membuat layanan perpustakaan digital tidak dapat diakses oleh pengguna yang sah, menyebabkan kerugian keuangan dan reputasi. Oleh karena itu, penting bagi perpustakaan digital untuk memahami berbagai ancaman ini agar mereka dapat mengambil tindakan keamanan yang tepat. Perpustakaan digital dapat memastikan keandalan dan kelancaran layanan informasi melalui pemantauan keamanan secara berkala, penggunaan enkripsi data, autentikasi dua faktor, dan edukasi pengguna tentang praktik keamanan *cyber*.

Implementasi Teknologi Keamanan

Implementasi teknologi keamanan menjadi landasan penting dalam upaya menjaga keamanan informasi dan privasi pengguna dalam layanan perpustakaan digital di tengah kondisi era yang semakin kompleks dan canggih dalam potensi ancaman keamanan. Dalam menghadapi tantangan ini, perpustakaan digital harus menerapkan solusi teknologi yang efektif dan inovatif, tidak hanya melindungi data sensitif pengguna, tetapi juga menjaga integritas dan ketersediaan sistem secara keseluruhan. Seperti yang diusulkan oleh Sayed et al. (2019), ada beberapa alternatif teknologi yang dapat digunakan untuk meningkatkan keamanan dan privasi data dalam konteks perpustakaan digital. Ini termasuk implementasi tiga lapisan untuk proses *login*, pengaturan yang menyembunyikan halaman *login* admin, penggunaan mekanisme penundaan autentikasi *password*, serta penerapan CAPTCHAS, verifikasi kode, dan *encoding* XSS Syntax untuk mengurangi potensi serangan dan melindungi data sensitif pengguna. Pada khususnya, penerapan tiga lapisan untuk proses *login*, dapat membantu mengurangi risiko serangan *cyber* dengan memperkuat sistem autentikasi dan menghalangi akses yang tidak sah ke data sensitif pengguna, sehingga meningkatkan tingkat keamanan dan privasi dalam layanan perpustakaan digital.

Ngwum et al. (2020) menyebutkan bahwa dalam menjamin keamanan dan privasi data perpustakaan digital, enkripsi serta autentikasi dan otoritasi merupakan aspek yang krusial. Enkripsi data melibatkan konversi data menjadi bentuk yang tidak dapat dibaca oleh pihak ketiga (yang dapat menjadi musuh potensial) dan pengembalian data yang sama ke bentuk asli yang dapat dibaca di ujung penerima atau sistem menggunakan kunci rahasia. Enkripsi dapat memastikan kerahasiaan data. Adanya enkripsi data memungkinkan perpustakaan digital dapat melindungi informasi sensitif seperti riwayat peminjaman, informasi akun pengguna, data identitas dari akses yang tidak sah, dan data lainnya. Data yang dienkripsi akan tetap aman bahkan jika disusupi oleh pihak yang tidak berwenang, karena pihak tersebut tidak dapat membaca atau memanipulasi informasi tanpa kunci enkripsi yang benar. Sedangkan, autentikasi adalah proses verifikasi identitas pengguna, yang memastikan bahwa orang yang mencoba mengakses sistem adalah orang yang seharusnya. Di sisi lain, otorisasi melibatkan kontrol akses yang tepat terhadap sumber daya atau informasi di dalam sistem berdasarkan identitas pengguna yang telah terautentikasi. Selain itu, otorisasi memungkinkan perpustakaan digital untuk mengontrol tingkat akses yang diberikan kepada setiap pengguna. Dengan menetapkan izin akses yang sesuai, perpustakaan dapat memastikan bahwa pengguna hanya memiliki akses ke informasi yang relevan dengan peran atau kebutuhan pengguna dalam sistem.

Singh et al. (2018) menggarisbawahi bahwa penggunaan *firewall* dapat menjadi salah satu alternatif yang efektif untuk menjaga keamanan data dalam konteks perpustakaan digital. *Firewall*, sebagai perangkat keamanan jaringan yang canggih, memiliki peran krusial dalam memantau dan mengontrol lalu lintas internet yang masuk dan keluar dari jaringan perpustakaan digital. Dengan fungsi utamanya sebagai penghalang pertama, *firewall* secara signifikan berkontribusi dalam melindungi jaringan perpustakaan dari berbagai serangan luar yang berpotensi membahayakan. Melalui kemampuannya dalam menganalisis lalu lintas data, *firewall* dapat secara efisien mendeteksi dan memblokir akses yang tidak sah, termasuk serangan *malware* dan serangan DDoS yang dapat merusak sistem perpustakaan digital. Selain itu, *firewall* juga memainkan peran penting dalam mengidentifikasi dan menghentikan serangan yang sedang berlangsung dengan cepat, sehingga membantu mengurangi risiko kerusakan dan kerugian yang mungkin ditimbulkan oleh serangan keamanan tersebut. Dengan demikian, penggunaan *firewall* bukan hanya sebagai langkah proaktif dalam mencegah serangan keamanan, tetapi juga sebagai elemen penting dalam strategi pertahanan perpustakaan digital untuk menjaga keamanan dan integritas data pengguna.

Pengaruh Regulasi dan Kebijakan Privasi dalam Layanan Perpustakaan Digital

Regulasi dan kebijakan privasi memiliki dampak yang sangat signifikan dalam pengelolaan keamanan informasi dan privasi pengguna dalam layanan perpustakaan digital. Sebagai bagian dari upaya untuk melindungi hak privasi individu dan memastikan integritas data, regulasi dan kebijakan privasi memberikan kerangka kerja yang jelas tentang bagaimana informasi pribadi harus ditangani oleh perpustakaan digital, termasuk proses pengumpulan, penyimpanan, penggunaan, dan pembagian data.

Salah satu dampak utama dari regulasi dan kebijakan privasi adalah meningkatnya tanggung jawab perpustakaan digital dalam melindungi data pengguna (Morehouse et al., 2020). Contoh yang menonjol adalah GDPR (*General Data Protection Regulation*) menetapkan standar yang ketat untuk pengumpulan, pengolahan, dan penyimpanan data pribadi, serta memberikan hak kepada individu untuk mengontrol dan mengakses informasi pribadi mereka. Studi yang dilakukan oleh Lund (2021) menunjukkan bahwa kebijakan privasi yang paling berhasil adalah kebijakan yang dibangun dari kerangka atau pedoman yang ada, seperti *Library Bill of Rights*. Kebijakan yang dibangun dengan memperhatikan pedoman seperti itu mampu memberikan detail yang ekstensif dan memperbolehkan kebebasan optimal kepada pengguna dalam mengontrol dan mengelola informasi pribadi mereka. Dengan demikian, kebijakan semacam itu memberikan landasan yang kuat bagi perpustakaan digital dalam upaya mereka untuk melindungi privasi dan keamanan data pengguna, sambil tetap memastikan bahwa akses terhadap informasi tetap terjaga dengan baik dalam lingkungan digital yang terus berkembang.

Secara ringkas, berikut merupakan analisis hasil dari rujukan berdasarkan aspek ancaman keamanan dan privasi dalam layanan perpustakaan digital, implementasi teknologi keamanan, serta pengaruh regulasi dan kebijakan privasi dalam layanan perpustakaan digital yang disajikan dalam Tabel 1.

Tabel 1. Analisis hasil rujukan penelitian berdasarkan aspek

Sumber Penelitian	Aspek yang dikaji	Temuan Penelitian
Pandey et al. (2021)	Ancaman keamanan dalam layanan perpustakaan digital	Kerusakan atau kerugian dalam berbagai cara mulai dari informasi kecil hingga kehancuran seluruh sistem.
Liu (2019)	Ancaman keamanan dalam layanan perpustakaan digital	Ancaman keamanan berupa peretasan virus, pencurian aku, dan penghancuran data.
Han et al. (2016)	Ancaman keamanan dalam layanan perpustakaan digital	Ancaman terhadap aset fisik (komputer-server, perangkat keamanan-*fireproof wall hardware*), ancaman serangan kata sandi dan kerentanan perlindungan kata sandi perangkat lunak, serangan *brute force*, *phishin*g
Yusuf et al. (2021)	Ancaman keamanan dalam layanan perpustakaan digital	Ancaman dalam aspek *hardware security*, *software security*, *network security*, *data security*, dan *physical and human threat*.
Sayed et al. (2019)	Implikasi teknologi keamanan	Alternatif untuk menjaga keamanan dan privasi data dalam aspek perpustakaan digital yang meliputi tiga lapisan untuk *login*, menyebunyikan halaman *login* admin, *password authentication delay*, menggunakan CAPTCHAS, verifikasi kode, menggunakan *encoding* XSS Syntax, *XSS using Script via Encoded URI Schemes*.
Ngwum et al. (2020)	Implikasi teknologi keamanan	Penjaminan keamanan dan privasi data perpustakaan digital dapat dilakukan melalui enkripsi serta autentikasi dan otoritasi data.

Sumber Penelitian	Aspek yang dikaji	Temuan Penelitian
Singh et al. (2018)	Implikasi teknologi keamanan	Penggunana *firewall* dalam menjamin keamanan dan privasi data.
Morehouse et al., (2020)	Pengaruh regulasi dan kebijakan privasi	Meningkatnya tanggung jawab perpustakaan digital dalam melindungi data pengguna.
Lund (2021)	Pengaruh regulasi dan kebijakan privasi	Kebijakan privasi yang paling berhasil adalah kebijakan yang dibangun dari kerangka atau pedoman yang ada, seperti *Library Bill of Rights*.

Dari hasil analisis tabel di atas, berbagai penelitian mengenai ancaman keamanan dan implikasi teknologi di layanan perpustakaan digital menunjukkan bahwa perpustakaan menghadapi beragam tantangan dalam menjaga keamanan informasi. Ancaman yang diidentifikasi meliputi peretasan, *malware*, pencurian data, serta kerentanan terhadap serangan *cyber* seperti *brute force dan phishing*, yang menekankan pentingnya perlindungan tidak hanya pada perangkat lunak, tetapi juga pada infrastruktur fisik. Selain itu, penerapan teknologi keamanan canggih seperti *enkripsi*, penggunaan *firewall*, dan autentikasi multi-lapis menjadi krusial untuk melindungi data pengguna. Penelitian juga menyoroti perlunya regulasi yang jelas dan kebijakan privasi yang efektif, yang sebaiknya didasarkan pada pedoman yang ada untuk memastikan kepatuhan dan efektivitas. Dengan demikian, kombinasi antara teknologi modern, pelatihan sumber daya manusia, dan kebijakan yang kuat sangat diperlukan untuk menciptakan lingkungan yang aman bagi pengguna perpustakaan digital.

Kesimpulan

Layanan perpustakaan digital telah menghadapi berbagai ancaman keamanan dan privasi, ancaman tersebut berupa seperti kerusakan atau kerugian data, peretasan virus, pencurian akun, dan kerentanan dalam perlindungan kata sandi. Untuk mengatasi ancaman ini, teknologi keamanan seperti enkripsi data, autentikasi, otorisasi, dan penggunaan *firewall* sangat penting. Selain itu, peraturan dan kebijakan privasi, seperti GDPR dan kebijakan berdasarkan kerangka atau pedoman yang ada, sangat penting untuk melindungi data pengguna yang menggunakan layanan perpustakaan digital. Untuk pengembangan penelitian selanjutnya, maka diperlukan analisis lebih lanjut tentang strategi teknologi keamanan yang dapat diterapkan, serta analisis tentang bagaimana peraturan dan kebijakan privasi dapat ditingkatkan untuk mengatasi tantangan yang ada.

Daftar Pustaka

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). Information security: A review of information security issues and techniques. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 1-6. https://doi.org/10.1109/CAIS.2019.8769504

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science.* https://doi.org/10.1177/01655515231160026

Han, Z., & Huang, S. (2016, June). Risk assessment of digital library information security: A case study. *The Electronic Library*, *34*(3), 471-487. https://doi.org/10.1108/EL-09-2014-0158

Hess, A. N., LaPorte-Fiori, R., & Engwall, K. (2015). Preserving patron privacy in the 21st century academic library. *The Journal of Academic Librarianship, 41*(1), 105-114. https://doi.org/10.1016/j.acalib.2014.10.010

Lund, B. D. (2021). Public libraries' data privacy policies: A content and cluster analysis. *The Serials Librarian, 81*(1), 99-107. https://doi.org/10.1080/0361526X.2021.1875958

Morehouse, S., Vitak, J., Subramaniam, M., & Liao, Y. (2020). Creating a library privacy policy by focusing on patron interactions. *In Sustainable Digital Communities: 15th International Conference, iConference 2020*, 571-578. https://doi.org/10.1007/978-3-030-43687-2_47

Nnatubemugo, N., Raina, S., Aguon, S., Taylor, B., & Kaza, S. (2020). A model for security evaluation of digital libraries: A case study on a cybersecurity curriculum library. *Journal of The Colloquium for Information Systems Security Education*, *7*(1), 1-12.

Pandey, P., & Misra, R. (2014, June). Digitization of library materials in academic libraries: Issues and challenges. *Journal of Industrial and Intelligent Information*, *2*(2), 136-141. https://doi.org/10.12720/jiii.2.2.136-141

Samonas, S., & Coss, D. (2014). The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3), 21-45.

Sayed, H., Elmahdy, H. N., Amer, F., & Shaheen, S. (2019). A novel framework to improve secure digital library at cloud environment. *International Journal of Computer Science and Information Security*, *17*(5), 13-22.

Setiono, Y., & Shintawati, Y. (2024). Studi kepustakaan: Keamanan data di perpustakaan digital. *Jurnal Perpustakaan dan Informasi*, *1*(1), 1-15.

Singh, V., & Margam, M. (2018, March). Information security measures of Libraries of Central Universities of Delhi: A Study. *DESIDOC Journal of Library & Information Technology, 38*(2), 102-109. doi: 10.14429/djlit.38.2.11879

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014, July). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*, *10*(7), 1-9. http://dx.doi.org/10.1155/2014/190903

Yusuf, A., Yusuf, S., & Zayyana, H. M. (2021). Assessment of information security threats to information systems in Federal University Libraries Nigeria. *Samaru Journal of Information Studies*, *21*(1), 38-47. https://www.ajol.info/index.php/sjis/article/view/217870

Yuying, L. (2019). Risk and preventive strategy of network security in university digital library. *9th International Conference on Management, Education and Information*, 133-137. https://webofproceedings.org/proceedings_series/ESSP/MEICI%202019/MEICI19026.pdf