Studi Kepustakaan: Keamanan Data Di Perpustakaan Digital

Yohanes Setiono[*)], Yanuastrid Shintawati[2]

[1]*Program Studi Ilmu Perpustakaan, Fakultas Hukum, Ilmu Sosial dan Ilmu Politik, Universitas Terbuka*
[2]*Departemen Ilmu Perpustakaan, Universitas Wijaya Kusuma Surabaya*

[*)] Korespondensi: yohanessetiono@gmail.com

Abstract

The digital library makes no guarantees on data security, whether it is about collections or personal information. The risks to information security in digital libraries are covered in this article, along with solutions. The purpose of this scholarly paper is to explore the hazards and methods for preventing digital library data security. This study is qualitative and relies on library research. This study makes use of library research. According to the research, physical objects used to hold information are also targeted by information security threats in digital libraries, in addition to information management programs or applications. Malware comes in a variety of forms and poses a threat to digital libraries' information security. Information that has been securely kept can be easily preserved by backing up (duplicating information). Backup is insufficient on its own, though. By including a variety of national and worldwide events, training managers, such as librarians, can perform better. In addition to human resources, updating the many technologies used in digital libraries is also necessary to prevent system disruptions. Additionally, digital libraries ought to periodically host information-conceding simulations so that, in the event of such unanticipated incidents, they can respond appropriately and limit the impact.

Keywords: Digital library; information security; their prevention

Abstrak

Perpustakaan digital tidak menjamin keamanan data, baik koleksi atau data pribadi. Penulisan artikel ilmiah ini bertujuan untuk membahas risiko dan cara mencegah keamanan data perpustakaan digital. Penelitian ini menggunakan studi pustaka (library research). Penelitian sebelumnya, pendapat ahli, dan sumber digital yang dipercaya oleh penulis dievaluasi dalam metode ini. Penelitian yang dilakukan, membuktikan bahwa risiko keselamatan data perpustakaan digital mencakup tidak hanya aplikasi atau program yang digunakan untuk mengatur data, tetapi juga objek fisik yang digunakan untuk mengarsip data. Malware berbagai jenis adalah salah satu contoh ancaman keamanan data perpustakaan digital. Back up (membuat atau menggandakan data) adalah cara paling mudah untuk memastikan data yang disimpan tetap aman. Namun, perlindungan satu-satunya tidak cukup. Penting bagi pustakawan dan pengelola lainnya untuk mendapatkan pelatihan yang lebih baik. Untuk mencegah gangguan sistem yang dijalankan, tidak hanya sumber daya manusianya, namun berbagai perangkat yang terlibat dalam perpustakaan digital juga harus diperbarui. Selain itu, perpustakaan digital harus rutin melakukan simulasi kebobolan informasi agar mereka dapat mengambil tindakan yang tepat saat peristiwa yang tidak diinginkan terjadi, sehingga efeknya tidak semakin meluas.

Kata kunci: Perpustakaan digital; perlindungan data; protektif

Pendahuluan

Dengan bantuan teknologi, perpustakaan telah berkembang pesat. Sebelumnya, perpustakaan identik dengan buku atau data di rak buku. Banyak perpustakaan sekarang menyimpan koleksi tercetaknya dalam bentuk digital. Pihak perpustakaan membuatnya mudah diakses, dan penggunanya tidak perlu pergi ke perpustakaan secara langsung. Ada sejumlah perpustakaan digital di Indonesia, tetapi istilah itu kurang tepat karena kebanyakan perpustakaan masih dipadukan dengan perpustakaan konvensional dan tidak benar-benar berfungsi sebagai perpustakaan digital (Triandari, 2022). Terlepas dari apakah istilah

"perpustakaan digital" digunakan secara tepat, setidaknya ada lebih dari lima perpustakaan di Indonesia yang menggunakan teknologi digital (Sayekti & Mardianto, 2019). Salah satu dari perpustakaan tersebut adalah *Indonesia Digital Library Network* (IDLN), sayangnya saat ini tidak tersedia. Perpustakaan lain adalah *Spektra Virtual Library* (SVL), tetapi situs webnya tidak dapat ditemukan saat penulis mencoba mengaksesnya (Haruddin & Suttaria, 2022).

Perpustakaan digital pasti terkait dengan teknologi, seperti yang ditunjukkan di atas. Teknologi sendiri berarti pengetahuan ilmiah yang digunakan untuk membuat sesuatu lebih baik, seperti membuat mesin atau perangkat yang memudahkan pekerjaan (Zulham, 2017). Nurhayati (2018) menyebutkan pendapat Federasi Perpustakaan Digital, pengertian perpustakaan digital adalah organisasi yang menyediakan berbagai sumber daya, termasuk sumber daya manusia atau staf ahli yang memiliki kemampuan untuk memilih, mengolah, dan menyediakan akses intelektual, kemudian menginterpretasikan, mendistribusikan, menjaga integritas profesi, dan memelihara koleksi digital secara berkelanjutan untuk dapat diakses oleh masyarakat umum dalam jangka Panjang. Pengamatan telah dilakukan oleh rivalina dan anwas mengenai peran TIK dalam perpustakaan. Hasil penelitian menunjukkan bahwa TIK dapat dengan mudah mengakses berbagai jenis informasi seperti teks, audio, video, dan multimedia di perpustakaan, terutama perpustakaan dengan basis digital. Selain itu, karena pengelolaan bahan pustaka menjadi lebih mudah dan profesi pustakawan menjadi lebih profesional, layanan perpustakaan semakin cepat dan lebih luas (Nasrullah, 2018). Namun, peran TIK, terutama di perpustakaan digital, juga memiliki kelemahan. Kelemahan sistem perlindungan data dapat menyebabkan perampasan data, pemotongan data, *hacking* (yang memungkinkan seseorang mengakses informasi secara tidak sah), joy computing (yang memungkinkan seseorang menggunakan komputer tanpa persetujuan), *data diddling* (yang mengedit data yang sah menjadi salah), dan ancaman lainnya untuk pengguna dan perpustakaan (Sari, 2023). Dibutuhkan pencegahan dan penanganan untuk mengurangi akibat ancaman tersebut.

Studi sebelumnya (Al-Suqri & Akomolafe-Fetuyi, 2014) melihat masalah keamanan dan privasi utama yang dihadapi perpustakaan digital, dan telah menekankan metode yang harus dilakukan untuk melindungi keamanan pengguna dan integritas lingkungan digital perpustakaan. Sudah jelas bahwa akan ada biaya. Pengelola perpustakaan digital harus memastikan bahwa mereka memiliki sumber daya yang memadai untuk solusi teknis perpustakaan digital serta untuk pelatihan profesional dan pendidikan pengguna. Kolaborasi profesional perpustakaan dalam negeri dan internasional dapat meningkatkan efisiensi dan efektivitas inisiatif yang relevan serta membantu membakukan pendekatan terhadap pengembangan perpustakaan digital dan masalah keamanan dan privasi yang terkait (Al-Suqri & Akomolafe-Fatuyi, 2014). Selain itu berdasarkan penelitian Nuansa & Rohmiyati, 2017 perlindungan keamanan perpustakaan mencakup keamanan fisik, penggunaan teknologi keamanan, dan penerapan kebijakan untuk mencegah penyalahgunaan bahan pustaka (Nuansa & Rohmiyati, 2017).

Wulandari & Nugroho, (2017) mengatakan bahwa perpustakaan virtual adalah perpaduan antara koleksi digital dan sistem informasi berbasis web atau elektronik. Berbeda dengan beberapa istilah yang telah disebutkan sebelumnya, istilah "perpustakaan internet", atau "perpustakaan internet", dimaksudkan

untuk perpustakaan yang memanfaatkan Internet untuk menyediakan akses dan layanan. Penelitian ini memiliki kesamaan dan perbedaan dengan studi sebelumnya. Salah satu hal yang menghubungkan penelitian ini dengan penelitian sebelumnya adalah diskusi tentang ancaman terhadap keamanan informasi, yang telah menjadi masalah sejak data tercetak di lembaga menjadi digital. Sementara perbedaan terletak pada fakta bahwa penelitian akan dilakukan lebih lanjut tentang risiko dan pencegahan privasi perpustakaan digital yang lebih spesifik, penulis menyarankan untuk melakukan penelitian lebih lanjut pada perpustakaan digital tertentu, seperti Ruang Buku Kominfo, hanya dari perspektif keamanan data.

Penelitian ini mengkaji sistem perlindungan dan privasi perpustakaan digital lebih lanjut. Penelitian ini juga membahas ancaman keamanan data perpustakaan digital, dan cara pustakawan dapat mencegah ancaman tersebut.

Metode

Studi ini menggunakan metodologi studi pustaka (*library research*). Penelitian menganalisis hasil penelitian ini secara digital tanpa melakukan tinjauan langsung ke lapangan, serta beberapa pendapat ahli dan sumber terpercaya lainnya. Sumber data penelitian berasal dari literatur artikel atau jurnal yang bisa diakses digital. Selain itu, ulasan literatur dapat didefinisikan sebagai presentasi tentang teori, hasil, dan bahan penelitian dari penelitian sebelumnya untuk digunakan sebagai acuan atau dasar untuk penelitian berikutnya (Narendra, 2014). Penelitian yang menerapkan pendekatan ini mungkin hanya menyalin temuan penelitian sebelumnya. Namun demikian, pemaparan penelitian yang dilakukan dengan metode ini mencakup penulisan pola penelitian serta penggabungan rangkuman dan analisis (Ramdhani et al., 2014). Menurut Ramdhani (2014), tujuan penelitian yang dilakukan dengan metode *review* literatur adalah untuk mempelajari seberapa besar kontribusi ilmuan yang telah dibuat untuk topik atau masalah yang akan diteliti (Ramdhani et al., 2014). Metode *review* literatur dalam penelitian ini, diharapkan penulis dapat mengetahui tentang masalah, keamanan informasi pada perpustakaan digital.

Penulis menggunakan Teknik pengumpulan data model literasi Empowering 8, metode untuk menyelesaikan masalah studi yang dibuat oleh IFLA, saat memilih literatur untuk dibahas dalam artikel ini (Bocken et al., 2014). Model literasi ini terdiri dari beberapa proses: menemukan (mengidentifikasi tema diskusi), menggali (menggali informasi tambahan tentang subjek), memilih (memilih data yang sesuai dengan tema), mengorganisir (mengelompokkan data yang telah dikumpulkan), membuat (membuat simpulan menggunakan bahasa pribadi dari data yang terkumpul), dan menyampaikan (mempersiapkan data yang telah terkumpul untuk dibagikan) (Bocken et al., 2014; Katulić et al., 2022). Data dari berbagai literatur artikel dianalisis secara kualitatif.

Hasil dan Pembahasan

1. Sistem Perlindungan Dan Privasi Data Di Perpustakaan Digital

Teknologi informasi dan komunikasi (tik) sangat penting untuk pendidikan. Perkembangan teknologi informasi mempengaruhi hampir semua tingkat pendidikan. Ini disebabkan oleh munculnya metode baru dan proses pembelajaran dalam dunia pendidikan. Teknologi ini memungkinkan apa yang sebelumnya tidak mungkin dicapai dengan pembelajaran konvensional. Tik menjadi sangat populer di bidang pendidikan saat ini sehingga banyak negara bersaing untuk menggunakannya dan menghabiskan sumber daya yang sangat besar. Pertama, gaya belajar generasi saat ini. Generasi dewasa ini yang lahir setelah tahun 2000an telah mengenal berbagai perangkat teknologi sejak lahir. Mereka dikenal sebagai generasi born digital atau generasi millenial, yang dilahirkan di era digital, dan pola belajar mereka menggunakan sumber daya digital. Kedua, format sumber daya pendidikan berubah. Perkembangan teknologi internet memungkinkan pertumbuhan sumber informasi yang sangat cepat dewasa ini (hakim, 2015).

Pembicaraan tentang perpustakaan digital, atau perpustakaan digital, sangat luas. Terlepas dari berbagai definisi yang telah diberikan oleh beberapa pakar di bidang ilmu perpustakaan dan teknologi informasi, istilah "perpustakaan digital" memiliki satu hal yang sama: menyimpan informasi digital, menyebarkan informasi melalui jejaring berbasis teknologi (*network*), dan menggunakan perangkat elektronik untuk mendapatkan akses ke informasi. Perpustakaan digital memiliki beberapa fitur. Dalam handbook perpustakaan digital secara keseluruhan, widiyawati (2019) menyatakan bahwa ada banyak tema yang berkaitan dengan perpustakaan digital. Pertama, perpustakaan digital mencakup seluruh siklus informasi. Ini termasuk mengumpulkan data saat dibuat, membuatnya tersedia, menyimpannya dan memliharanya sehingga bermanfaat bagi komunitas pengguna, dan kadang-kadang membuangnya. Kedua, cakupan konten digital saat ini lebih luas dan mencakup sumber primer seperti statistik, data sesnsus, dokumen arsip, dan lain-lain. Ketiga, koleksi perpustakaan harus tetap sesuai. Perpustakaan digital, katalog, pangkalan data indeks dan abstak, dan terkadang termasuk isi artikel jurnal. Koleksi digital dapat dibangun dalam dua cara utama dari perspektif konten digital: membeli koleksi digital dalam bentuk buku atau jurnal elektronik; dan memindai koleksi cetak yang ada menjadi versi digital menggunakan perangkat pemindai. Cara pertama biasanya digunakan oleh perpustakaan untuk membuat koleksi elektronik berupa buku dan jurnal elektronik. Perpustakaan biasanya menggunakan metode ke dua untuk mengembangkan koleksi abu-abu, atau literatur hitam, di mana skripsi, tesis, dan hasil penelitian dialih-mediakan ke dalam bentuk digital dan disajikan secara digital.

Sistem keamanan informasi perpustakaan digital, seperti yang dijelaskan oleh ajagbomogun dalam artikel yang ditulis oleh erlianti (2017), adalah "sistem yang melindungi koleksi perpustakaan dari kejahatan seperti kerusakan dan pencurian". Dalam hal perpustakaan digital, sistem keamanan informasi yang dimaksudkan harus dapat melindungi semua koleksi digital perpustakaan, termasuk gambar dalam format jpg, png, atau format lainnya, serta koleksi digital audio dan video (erlianti, 2017). Perpustakaan digital adalah istilah yang mengacu pada penggunaan teknologi informasi sebagai cara untuk

menyimpan, mendapatkan, dan menyebarluaskan informasi ilmu pengetahuan dalam bentuk digital. Secara sederhana, kata "perpustakaan digital" mengacu pada tempat di mana koleksi informasi perpustakaan telah disimpan dalam bentuk digital (fitri, 2020). Tahun 2020, sni iso/iec 27001 ditetapkan sebagai standar untuk sistem manajemen keamanan informasi (smki) di indonesia oleh badan standardisasi nasional (bsn). Sni baru ini mengadopsi sistem keamanan informasi iso/iec 27001:2013 yang dikeluarkan oleh *international organization for standardization* (iso) dan *international electrotechnical commission* (iec). Sistem ini digunakan untuk menjaga, melindungi, melaksanakan, memantau, menganalisis, dan memelihara data yang dikumpulkan (bsn, 2014). Menurut laporan kinerja pusat data dan sistem informasi (pusdatin), penerapan sni iso/iec 27001:2013 berjalan dengan baik. Hasil penilaian kepatuhan dan sosialisasi sni iso/iec 27001:2013 yang dilakukan bsn di berbagai perguruan tinggi di indonesia memiliki nilai yang tinggi (akbar et al., 2020).

Oleh karena itu, pengelola data atau pustakawan bertanggung jawab atas keamanan informasi. Orang yang jujur harus memasang, mengelola, dan menghubungkan jaringan. Mengatur sistem file dan jaringan agar pengguna dapat mengaksesnya adalah tugas yang harus dilakukan oleh administrator. Memahami seluk beluk, memasang sistem pengaman, menjalankan program, dan membuat kata sandi masalah jaringan adalah tanggung jawab mereka. Mereka juga yang merancang dan menyimpan informasi untuk digunakan saat terjadi masalah.

2. Sistem Ancaman Keamanan Data Di Perpustakaan Digital

Perpustakaan digital bukan hanya penyimpanan umum, tetapi juga data pengguna dan pemustaka karena perubahan format data dari cetak ke non cetak. Ini karena untuk memiliki akses ke konten, pemakai harus menuliskan formulir atau menunjukkan kepribadian mereka (Unyil, 2018). Perpustakaan digital dapat menawarkan jasa seperti memobilisasi data kepribadian pemakai seperti lokasi, memantau penggunaan jasa, dan sebagainya. Menurut Pernyataan IFLA tentang Privasi di Lingkungan Perpustakaan (Hariyanti, 2017). Tahun 2013 dan 2014, Majelis Umum PBB telah memberitahukan pengumuman kebijakan privasi untuk semua negara, yang melibatkan penghormatan dan perlindungan hak privasi, seperti dalam komunikasi digital. Resolusi mengenai hak kebebasan di era digital adalah dasar dari pernyataan ini. Karena itu, perpustakaan digital dapat memilih jenis data individu yang diperoleh oleh pemakai (Hutahaean, 2015). Selain itu, mereka dapat meminta penyedia jasa komersial untuk melindungi data pemakai atau menolak jasa yang berlebihan jika hal itu dapat menyebabkan bahaya bagi data pemakai. Namun, perpustakaan mungkin tidak cukup memahami bagaimana layanan komersial atau lembaga pemerintah menangani data pribadi pengguna. Apakah data di perpustakaan yang menggunakan teknologi internet, koleksi atau data pemakai, benar-benar aman? (Utomo, 2021).

Pada prinsipnya, dunia maya sendiri tidak terjaga. Dunia maya adalah tempat dilakukannya kejahatan paling sering. Sangat mudah bagi pelaku untuk melihat data yang datang dan pergi melalui jaringan. Perpustakaan digital sering menggunakan program yang tidak aman, termasuk *server web* dan surat elektronik (Kurniawan et al., 2021). Salah satu cara paling mudah untuk memastikan bahwa data Anda aman di internet adalah dengan memastikan bahwa Anda menggunakan komputer Anda sendiri.

Ini dapat dicapai melalui pembatasan portal ke komputer Anda, seperti menggunakan gelar pengguna dan kode rahasia (Rahmah, 2018). Untuk menambah atau mengurangi jumlah informasi yang dikumpulkan pada komputer yang digunakan oleh banyak pengguna, diperlukan orang yang memiliki otoritas untuk melakukannya. Namun, risiko yang terkait dengan penggunaan komputer ini dapat berasal dari sumber dalam dan luar. Pusat bahaya lokal tidak terbatas pada pustakawan; mereka juga dapat berasal dari mitra, konsultan, vendor, kontraktor, dan anggota staf lainnya yang bertanggung jawab untuk mengorganisasikan perpustakaan digital (Chazar, 2015). Sebaliknya, pesaing perpustakaan digital yang mengganggu sistem perpustakaan digital merupakan contoh sumber bahaya eksternal.

Menurut Winata (2019), menjelaskan bahwa komputer yang dipakai dalam perpustakaan digital tidak dapat dianggap terlindungi karena virus dan *cybercrime* (kejahatan dunia maya) dapat terjadi. *Cybercrime* mencakup setidaknya lima tindakan, yaitu prampasan data, pemakaian komputer tanpa persetujuan, pengaksesan tidak sah, pengubahan data yang sah menjadi ilegal, dan penghancuran data penting sehingga data rusak dan tidak dapat dipakai (Samad, 2014). Menurut Rauf dkk., (2022), tindak kejahatan dalam dunia maya dapat dilakukan karena unjuk gigi atau bahkan kepentingan komersial. Pelaku biasanya memiliki tujuan unik untuk mengambil data pengguna, seperti untuk marketing.

Karena perpustakaan digital didistribusikan melalui sistem jaringan komputer, ancaman terhadap komputer ini semakin sulit untuk diatasi. Hal ini menunjukkan bahwa informasi dipindahkan antar komputer. Jika pengelolaan akses dibatasi pada komputer pusat, maka akses dapat dikontrol secara lokal. Namun semua data yang disimpan di semua komputer akan mengalami kendala jika komputer pusat yang berfungsi sebagai tempat penyimpanan mengalami kendala (Azmir & Wijayanti, 2022). Repositori adalah lokasi digital tempat berbagai aplikasi atau program diproses (Narendra, 2014). Pencatat *keystroke, virus, Trojan horse, worm, awareness, spyware, pornware*, dan pencurian kata sandi hanyalah beberapa contoh perangkat lunak berbahaya yang dapat diinstal pada komputer dan melancarkan serangan terhadap mesin (Prathivi & Vydia, 2017).

Malicious software, perangkat lunak yang berpotensi membahayakan sistem komputer disebut sebagai *malware*. *Malware* dibagi menjadi tiga kelompok berdasarkan tujuan pembuatannya (Situmorang et al., 2022). Kelompok pertama adalah *malware* yang terdiri dari virus dan worm yang bertujuan untuk menginfeksi program komputer. Dalam teknologi informasi, suatu program yang mereplikasi dirinya untuk menargetkan program komputer lain disebut virus (Tjahjadi & Santoso, 2023). Virus tidak hanya menargetkan program komputer, namun juga dapat menghasilkan iklan, mencuri informasi, dan bahkan mencuri uang. *Worm* adalah program komputer yang dapat mereplikasi dirinya sendiri untuk menargetkan program komputer lain, seperti virus. *Worm* dan virus berbeda dalam cara mereka menyebar. *Worm* dapat memperbanyak diri secara mandiri jika virus membutuhkan bantuan manusia (Tjahjadi & Santoso, 2023)

Malware jenis kedua bertujuan untuk bersembunyi di komputer atau berlindung. Jenis *malware* ini termasuk kuda *Trojan* dan *backdoor.* Keduanya adalah perangkat lunak yang diizinkan untuk diunduh. Seharusnya tidak ada masalah karena legal. Salah satu masalahnya adalah *trojan* yang diunduh ini

seringkali membawa virus, yang pada akhir-akhir ini mampu memberikan penyerang akses jarak jauh (Zhang et al., 2022). Namun, program yang dikenal sebagai *backdoor,* juga dikenal sebagai "pintu jebakan", memiliki kemampuan untuk memblokir sistem pengamanan komputer, memungkinkan pencuri untuk memasuki aplikasi komputer tanpa sistem perlindungan umumnya (Cahyanto et al., 2017). *Spyware, adware, bot, root kit, ransomware*, dan *malware* lainnya yang bertujuan untuk mengambil keuntungan dari program komputer termasuk dalam kelompok malware ketiga (Rathee & Garza-reyes, 2020).

"*Spy*" pada dasarnya berarti memata-matai. *Spyware* adalah program yang mengamati aktivitas komputer yang ditargetkan dan kemudian menyampaikan data ini kepada penyerang. Program ini juga dapat melakukan tugas tambahan, seperti mengganggu jaringan internet dan merusak sistem pengamanan komputer (Tjahjadi & Santoso, 2023). *Adware* adalah program yang bertujuan untuk tampil iklan dalam program (Komatwar & Kokare, 2021). Meskipun adware tidak menghasilkan uang bagi kita, *adware* adalah bisnis yang sangat menguntungkan bagi *advertiser*; lebih banyak orang yang melihat iklan, lebih banyak uang yang dihasilkan. (Agrawal et al., 2014). *Adware* yang dikombinasikan dengan *spyware* menjadi lebih berbahaya bagi komputer karena selain menampilkan iklan yang dimaksudkan untuk menghasilkan uang bagi penjahat, Selain itu, mereka dapat mengambil data dan mengawasi aktivitas pemakai. (Catak et al., 2020).

Bot adalah singkatan dari "*robot*", yang berarti suatu program komputer yang dapat melakukan tugas tertentu. *Bot* dibuat untuk merusak tujuan seperti komputer tanpa diketahui pemiliknya (Ilhamdi & Kunang, 2021). Contoh malware yang dapat digunakan secara legal adalah balasan otomatis ke *WhatsApp* atau pesan *email*, pemrograman video, konten digital, dan lainnya (Situmorang et al., 2022). Namun, *bot* ini juga berpotensi merusak jaringan komputer, ini menunjukkan bahwa komputer yang terhubung dengan *bot* lainnya juga akan mengalami masalah (Agrawal et al., 2014).

Rootkit adalah malware yang saling menfhubungkan dengan sistem perlindungan komputer dan hampir mirip dengan *backdoor*. Di sisi lain, *backdoor* memblokir sistem keamanan komputer, sementara *rootkit* adalah *software* atau kode yang digunakan untuk menyembunyikan file, registries, dan kode modul agar sistem keamanan komputer tidak dapat mendeteksi program *intrusion*, dan jenis file lainnya (Nugraha, dkk., 2019). Tujuan utamanya adalah untuk mencegah pengguna mengidentifikasi penyerang (Putri, dkk., 2022). *Malware* yang sangat berbahaya termasuk dalam *rootkit* ini karena memiliki kemampuan untuk mengambil alih sistem secara keseluruhan. Penghapusan dari komputer sangat bergantung pada metode manual karena kemanjuran *rootkit* (Situmorang et al., 2022). Ini berarti memperbaiki *rootkit* harus dilakukan oleh manusia, bukan sistem otomatis.

Ransomware adalah program yang merusak komputer dengan mengunci file. Jika orang ingin mengakses file tersebut lagi, mereka harus membayar ke alamat yang diminta. (Cahyanto et al., 2017). Berkas dengan format seperti *doc,. txt,. ppt,. jpeg,. zip,. pdf,. cgi, mdb,.db1,.dbx,.rft,.dsw,.cbm,.cpp,.asm,.gzip,.key*, dan *.pgp* biasanya menjadi target *ransomware* (Bastian, 2021). *Ransomware* tidak dapat dikeluarkan dari sistem dan pembayaran tidak menjamin

kembalinya file (Imaji, 2019). Ada kasus nyata *ransomware* yang menyerang perpustakaan digital. Perpustakaan Umum St. Louis, Amerika Serikat, mengalami peretasan pada tahun 2017. Perpustakaan Umum Kota St. Louis diminta untuk memberikan beberapa *bitcoin* kepada *hacker,* yang ditolak untuk membuka server yang diretas. Ini dilakukan karena, menurut penyelidikan FBI, *bitcoin* adalah mata uang digital yang sulit dilacak. Hasilnya, perpustakaan menghapus sistem komputer secara keseluruhan, yang kemudian perlu dibuat ulang dalam waktu singkat (Umar et al., 2021).

Semua data pengguna aman karena tidak disimpan di server. Namun, kasus ini menunjukkan bahwa perpustakaan digital dapat dibobol. Untuk mengatasi *ransomware* ini, pustakawan harus memiliki keahlian dalam mengoperasikan sistem komputer dan memastikan sistem selalu diperbarui. *Phishing*, yang berasal dari kata "memancing", adalah ancaman keamanan informasi berikutnya. berusaha "memancing" orang lain untuk secara sukarela memberikan data pribadinya tanpa sepengetahuan pemilik data (Prawira et al., 2023). Menurut data yang diambil dari situs web resmi *Ministry of Finance* Republik Indonesia, *ransomware, phishing,* dan *cryptocurrency* adalah ancaman keamanan data paling umum di tahun 2023.

3. Pencegahan Ancaman Keamanan Data Di Perpustakaan Digital

Organisasi paling sering menggunakan *backup* atau cadangan data untuk mencegah kehilangan data. Namun, hanya *backup* tidak cukup. Dalam penelitian Hanafiah (2023), menyatakan bahwa enkripsi, penggunaan *password, scanning fingerprint, watermarking, digital signatures,* sistem deteksi duplikat, dan sistem pembayaran adalah beberapa cara untuk melindungi informasi teknologi. Sebutan "enkripsi" berasal dari bahasa Yunani, "kriptos", yang berarti "tersembunyi". Enkripsi, atau yang dalam Bahasa Indonesia disebut enkripsi, adalah proses menggunakan algoritma enkripsi (*Bassel*) untuk mengubah bentuk pesan dari *plaintext* (pesan yang dapat dipahami orang) berubah menjadi *ciphertext* (pesan yang tidak dapat dipahami orang) (Firdaus & Jatmiko, 2019). Kunci yang hanya dapat dimiliki oleh pihak yang berwenang, diperlukan untuk mengubah pesan ke bentuk awalnya, atau plaintext. Sehingga, jika ada orang yang ingin membaca isi pesan, maka tidak akan dapat melakukannya jika tidak memiliki kunci yang dimaksud. Penggunaan kata sandi pada komputer, ATM, dan *e-commerce* adalah contoh enkripsi ini di dunia nyata (Pradypta, 2022).

Selain itu, memanfaatkan kata sandi dapat membantu mencegah kehilangan informasi; namun, *hacker* yang mahir dapat dengan mudah menemukan password dengan mengira data pemakai atau mengetahui kebiasaan mereka (Hatzivasilis, 2020). Di antaranya, dia mengatakan bahwa beberapa pola kata sandi yang harus dihindari untuk memastikan data Anda aman:

1. Kata-kata yang memiliki angka tambahan tidak kompleks (seperti dewi345, subhan56, alif09)
2. Kata-kata yang memiliki simbol tidak kompleks (seperti surya@an, m@nadya@ing, k@eyw0rd)
3. Kata-kata atau karakter bersambung (seperti kankan, ddeeefff, 69696969)
4. Jika menggunakan kata sandi, harus menghindari data pribadi pengguna seperti tanggal lahir, nama pasangan, dan lokasi tinggal.

Pemindaian sidik jari adalah pendekatan tambahan dapat digunakan untuk tujuan yang sama. seperti penggunaan kata sandi.

Watermark memiliki tujuan berbeda dari *encryption* dan kata sandi, yaitu menjaga kemurnian surat. *Watermarking*, menurut Azzura, dkk. (2023), adalah metode untuk memasukkan data ke dalam komponen multimedia seperti foto, video, dan musik. Data yang dimasukkan harus dapat diidentifikasi oleh media yang menyertainya. Ada banyak jenis teknik penyisipan data, tetapi yang paling umum adalah *watermarking* gambar, yang bertujuan untuk melindungi gambar aslinya. Salah satu contoh *watermarking* adalah ketika sebuah gambar diunduh dari internet dan terdapat tulisan atau logo yang mengidentifikasi pemilik gambar tersebut (Fathiha, 2021).

Penggunaan tanda tangan digital, seperti *watermarking,* juga berfungsi untuk melindungi plagiasi dan kemurnian data. Tanda tangan digital dapat digunakan untuk memverifikasi atau membuktikan apakah informasi yang dikirim telah diubah. Selain itu, akan mudah untuk diminta pertanggungjawaban jika dokumen terbukti diubah dengan tanda tangan (Hutahaean, 2015). Sistem pengenalan duplikat berbeda.Sistem deteksi peniruan ini dirancang untuk mencegah karya orang atau organisasi dipijak. Deteksi plagiarisme sangat mudah untuk mengidentifikasi plagiarisme apa pun oleh seseorang, termasuk foto, video*, drawing*, menulis, dan lainnya. Plagiarisme adalah masalah besar dalam pendidikan dan penerbitan ilmiah (Nguyen & Nguyen, 2015). Selain itu, algoritma mungkin saja sistem ini tidak dapat mengembalikan transformasi parameter yang tepat jika konten salinan berubah secara keseluruhan (Allili et al., 2019).

Ada cara lain untuk melindungi data Anda selain yang disebutkan di atas, seperti menggunakan sistem pembayaran. Mungkin pada awalnya, sistem pembayaran ini mirip dengan *ransomware.* Namun keduanya sangat berbeda, terutama dalam hal kepemilikan dan operasi mereka. Seperti yang disebutkan sebelumnya, *ransomware* membatasi akses data pengguna. Mereka harus membayar sejumlah uang yang diminta untuk mendapatkan akses kembali. Ini menunjukkan bahwa pengguna memiliki kendali atas data mereka. Namun, orang lain memiliki akses ke data pengguna dan ingin mereka membayar tebusan. Meskipun pihak yang melakukan penguncian akses mungkin tidak terlalu tertarik dengan data pengguna, pihak tersebut mungkin juga sangat tertarik dengan data tersebut. Meskipun pengguna membayar, akses tidak akan dikembalikan.

Tidak seperti sistem pembayaran, di mana pengguna tidak memiliki informasi yang diperlukan. Sebaliknya, mereka harus membayar kepada orang yang memiliki informasi tersebut agar mereka dapat mengaksesnya. Pembayaran ini berfungsi sebagai jaminan bahwa, setelah pembayaran selesai, pengguna akan dapat mengakses informasi yang diinginkannya. Jika ini tidak terjadi, penggun Sari (2023) menambahkan tiga saran tambahan dari tujuh cara yang telah dijelaskan sebelumnya untuk mencegah ancaman terhadap informasi: meningkatkan profesionalisme pustakawan dengan mengikuti kursus keamanan data; selalu membuat file dan terus meningkatkan *hardware* dan *software facilities* cadangan.

Seorang pustakawan harus memiliki empat belas kemampuan (kemampuan) untuk menjadi profesional di era digital (Hariyanti, 2017). Empat belas kemampuan tersebut adalah sebagai berikut:

1. Desain dan manajemen *database* yang unggul
2. Pengelolaan data *warehousing*
3. Memahami proses penerbitan elektronik
4. Pengetahuan tentang *hardware*
5. Arsitektur informasi yang unggul
6. Sumber informasi yang unggul
7. Integrasi informasi
8. Desain intranet dan ekstranet yang unggul
9. Pengembangan aplikasi *software* yang unggul
10. *Programming*
11. *Workflow* (alur kerja)
12. Memahami pengolahan teks
13. Mengendalikan meta data
14. Menguasai perangkat lunak untuk manajemen informasi

IFLA (2021) juga menyebutkan sepuluh hal yang harus dilakukan oleh pustakawan perpustakaan digital untuk menjadi lebih profesional, dan lima di antaranya berfokus pada keamanan informasi. Salah satu aspek yang disebutkan adalah pemeriksaan keamanan *cyber*, dimana dijelaskan bahwa pustakawan yang bekerja di perpustakaan digital harus mengenkripsi data yang dikirimkan melalui internet dan selalu memastikan bahwa komputer yang digunakan selalu *up-to-date*. Terkadang terjadi kejadian yang tidak diinginkan seperti kebocoran data, meskipun telah dilakukan segala upaya untuk memastikan keamanan data. Apa yang harus dilakukan jika kebobolan keamanan data terjadi? Untuk mencegah kebobolan keamanan informasi, organisasi harus selalu mengikuti enam langkah (Mz, 2021) yaitu:

1. Kaji kerusakan yang terjadi.
2. Usahakan agar kerusakan tidak meluas, salah satu caranya adalah dengan memblokir jaringan sistem.
3. Catat kejadian tersebut secara tertulis, termasuk akun yang disusupi, sistem yang terkena dampak, layanan yang terganggu, data dan jaringan yang terkena dampak, serta jumlah dan jenis kerusakan.
4. Libatkan penegak hukum.
5. Beri tahu orang-orang jika ada insiden yang membahayakan informasi mereka.
6. Mengambil pelajaran dari peristiwa tersebut untuk mencegahnya terjadi lagi di kemudian hari.

Simpulan

Sebagai hasil dari penelitian ini, sistem perlindungan dan privasi perpustakaan digital membuktikan bahwa data tidak selalu aman. Ada banyak ancaman yang dapat merusak atau bahkan menghapus data. Tahun 2023 dikatakan, ancaman terbesar keamanan data adalah *ransomware, phishing,* dan

cryptocurrency. Oleh karena itu mempelajari cara menggunakan komputer, *software*, *programming*, dan duplikasi data, baik di dalam maupun di luar negeri, staf yang mengelola *digital libraries* diharapkan dapat menjadi lebih profesional. Mereka juga harus secara teratur meninjau semua aset mereka dan memperkirakan potensi bahaya yang akan datang. Namun, berbagai perangkat yang digunakan di *libraries* harus diperbarui selain meningkatkan kinerja manusia. Ini dilakukan untuk memastikan bahwa sistem yang sedang dijalankan tidak tertinggal dari sistem yang digunakan para *hacker.*

Perpustakaan digital di Indonesia dapat menerapkan SNI ISO/IEC 27001 sebagai sistem keamanan informasi. Selain itu, perpustakaan digital harus melakukan simulasi kebobolan informasi secara berkala. Ini dilakukan agar perpustakaan dapat mengambil tindakan yang tepat saat peristiwa yang tidak diharapkan ini terjadi, sehingga dampak yang terjadi tidak semakin meluas. Selanjutnya, penelitian perlu dilakukan tentang ancaman dan manajemen keamanan data di perpustakaan digital tertentu, seperti Ruang Buku Kominfo.

Daftar Pustaka

Agrawal, M., Singh, H., Gour, N., & Kumar, A. 2014. Evaluation on Malware Analysis. *International Journal of Computer Science and Information Technologies*, *5*(3), 3381–3383.

Akbar, R. M., Utomo, A. T. S., & Haeroni, Y. P. 2020. Perancangan Disaster Recovery Plan (DRP) untuk Meningkatkan Ketersediaan Layanan Sistem Pemerintahan Berbasis Elektronik (SPBE) pada Badan Standardisasi Nasional. *Pertemuan Dan Presentasi Ilmiah Standardisasi*, *2019*, 283–290. https://doi.org/10.31153/ppis.2019.31

Al-Suqri, M. N., & Akomolafe-Fatuyi, E. 2014. Security and Privacy in Digital Libraries: *International Journal of Digital Library Systems*, *3*(4), 54–61. https://doi.org/10.4018/ijdls.2012100103

Allili, M., Casemajor, N., & Talbi, A. 2019. Multiple image copy detection and evolution visualisation using tree graphs. *Multimedia Tools and Applications*, *78*. https://doi.org/10.1007/s11042-018-6350-5

Azmir, A. F., & Wijayanti, L. 2022. Cloud Computing Opportunities and Challenges in Electronic Document Management. *Record and Library Journal*, *8*(2), 248–258. https://doi.org/10.20473/rlj.v8-i2.2022.248-258

Azzura, C. M., Pratiwi, M., & Desyanti, D. 2023. Implementasi Watermarking Desain Citra Menggunakan Metode Modifikasi End Of File (MEOF). *JUTEKINF (Jurnal Teknologi Komputer dan Informasi), 11*(1), 1-9. https://doi.org/10.52072/jutekinf.v11i1.473

Bastian, A. 2021. Improving Antivirus Signature For Detection Ransomware Attacks With Machine Learning. *Smart Comp :Jurnalnya Orang Pintar Komputer*, *10*(1), 30–34. https://doi.org/10.30591/smartcomp.v10i1.2190

Bocken, N. M. P., Short, S. W., Rana, P., & Evans, S. 2014. A literature and practice review to develop sustainable business model archetypes. *Journal of Cleaner Production*, *65*(September), 42–56.

https://doi.org/10.1016/j.jclepro.2013.11.039

Cahyanto, T. A., Wahanggara, V., & Ramadana, D. 2017. Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis. *Jurnal Sistem & Teknologi Informasi Indonesia*, *2*(1), 19–30.

Catak, F. O., Yazi, A. F., Elezaj, O., & Ahmed, J. 2020. Deep learning based Sequential model for malware analysis using Windows exe API Calls. *PeerJ Computer Science*, *6*, 1–23. https://doi.org/10.7717/PEERJ-CS.285

Chazar, C. 2015. Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005. *Jurnal Informasi*, *VII*(2), 48–57.

Erlianti, G. 2017. Penerapan Sistem Keamanan Koleksi Pada Perpustakaan Kota Yogyakarta. *Shaut Al-Maktabah : Jurnal Perpustakaan, Arsip Dan Dokumentasi*, *9*(1), 115–124.

Fathiha, V. A. 2021. Implementasi Teknik Watermarking 4Menggunakan Metode Discrete Wavelet Transform (DWT) dan Singular Value Decomposition (SVD) pada Citra Digital. *Jurnal Ilmiah Teknologi Informasi Asia*, *14*(2), 125. https://doi.org/10.32815/jitika.v14i2.262

Firdaus, Z., & Jatmiko, D. A. 2019. Implementasi Algoritma Advanced Encryption Standard (Aes) Sebagai Sistem Pengamanan Data Pengarsipan Pada Perpustakaan Digital Di Puslitbang Geologi …. *Elibrary.Unikom.Ac.Id*. https://elibrary.unikom.ac.id/id/eprint/1350/

Fitri, M. O. 2020. Rancangan Perpustakaan Digital Berbasis Web Fakultas Sains dan Teknologi UIN Imam Bonjol Padang dengan Menggunakan Omeka. *Teknosains: Media Informasi Sains dan Teknologi*, *14*(2), 128-136. https://doi.org/10.24252/teknosains.v14i2.14451

Hakim, H. A. B. 2015. Internet dan Kapitalisme Informasi di Perpustakaan. *Info Persadha*, *13*(2), 2-12. http://e-journal.usd.ac.id/index.php/Info_Persadha/article/view/1

Hanafiah, M. 2023. Penerapan Algoritma SHA-384 Pada Aplikasi Duplicate Video Scanner. *Bulletin of Data Science, 2*(2), 81-88. https://ejurnal.seminar-id.com/index.php/bulletindsMuhammad

Hariyanti. 2017. *Peran Perpustakaan dan Pustakawan Politeknik Kesehatan Semarang dalam Penyediaan Sumber Informasi untuk Mendukung Gerakan Masyarakat Hidup Sehat*. *6*(2), 1–9.

Haruddin, H., & Suttaria, S. 2022. Strategi Pengembangan Perpustakaan Digital UIN Alauddin Makassar. *LIBRARIA: Jurnal Perpustakaan*, *10*(2), 313. https://doi.org/10.21043/libraria.v10i2.15230

Hatzivasilis, G. 2020. Password management: How secure is your login process? *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12512 LNCS*(March), 157–177. https://doi.org/10.1007/978-3-030-62433-0_10

Hutahaean, Jeperson. 2015. *Konsep Sistem Informasi*. Yogyakarta : Deepublish Publisher.

Ilhamdi, Y., & Kunang, Y. N. 2021. Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik. *In Bina Darma Conference on Computer Science* (BDCCS), *3*(2), 256-264. https://conference.binadarma.ac.id/index.php/BDCCS/article/download/2124/897

Imaji, A. O. 2019. *Ransomware Attacks: Critical Analysis, Threats, and Prevention methods Asibi O. Imaji Fort Hays State University March 5, 2019*. *March*.

Katulić, A., Katulić, T., & Hebrang Grgić, I. 2022. Application of the principle of transparency in processing of European national libraries patrons' personal data. *Digital Library Perspectives*, *38*(4), 399–411. https://doi.org/10.1108/DLP-11-2021-0097

Komatwar, R., & Kokare, M. 2021. A Survey on Malware Detection and Classification. *Journal of Applied Security Research*, *16*(3), 390–420. https://doi.org/10.1080/19361610.2020.1796162

Kurniawan, R., Alhakim, A., Safero, B., Valeria, J., Angelina, S., Internasional Batam, U., Gajah Mada, J., -Sei Ladi, B., & Riau, K. 2021. Penggunaan Internet yang Sehat dan Aman di Kalangan Masyarakat dan Pelajar. *Jurnal ABDIMASA Pengabdian Masyarakat*, *4*(2), 15–21.

Mz, M. A. 2021. Cobit 5 Untuk Tata Kelola Audit Sistem Informasi Perpustakaan. *Jurnal Teknoinfo*, *15*(2), 67-73. https://doi.org/10.33365/jti.v15i2.1078

Narendra, A. P. 2014. PERPUSTAKAAN DIGITAL DAN REPOSITORI INSTITUSI UNIVERSITAS (SHARING PENGALAMAN DI UNIKA SOEGIJAPRANATA SEMARANG) Al . Pramukti Narendra Staf Perpustakaan Unika Soegijapranata Semarang Email : albertopramukti@yahoo.com. *Persadha*, *12* no *1*.

Nasrullah. 2018. Penerapan Teknologi Informasi dan Komunikasi di Perpustakaan. *Diskusi Ilmiah*, 1–8. https://idr.uin-antasari.ac.id/10639/

Nguyen, L. H., & Nguyen, T. O. 2015. A copy detection method. *ACM International Conference Proceeding Series*, *03-04-Dece*(December 2015), 111–115. https://doi.org/10.1145/2833258.2833268

Nuansa, G., & Rohmiyati, Y. 2017. Evaluasi Sistem Keamanan Perpustakaan Bagi Perlindungan Koleksi Di Perpustakaan Provinsi Jawa Tengah. *Jurnal Ilmu Perpustakaan*, *6*(3), 501–510. https://ejournal3.undip.ac.id/index.php/jip/article/view/23182

Nugraha, J. D., Budiyono, A., & Almaarif, A. 2019. Analisis Malware Berdasarkan API Call Memory Dengan Metode Deteksi Signature-Based. *eProceedings of Engineering, 6*(2), 7820-7827 https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/10639

Nurhayati, A. 2018. Perkembangan perpustakaan dalam pemenuhan kebutuhan informasi masyarakat. *UNILIB: Jurnal Perpustakaan*, *9*(3), 23-34. https://doi.org/10.20885/unilib.vol9.iss1.art3

Pradypta, A. A. 2022. Perancangan Aplikasi Data Security Dalam Melindungi Informasi Digital Menggunakan Teknik Algoritma Rijndael Berbasis Desktop. *Jurnal Maklumatika*, *9*(1), 68–76. https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/141%0Ahttps://maklumatika.i-tech.ac.id/index.php/maklumatika/article/download/141/138

Prawira, D., Nugraha, B., & Marzuki, M. I. 2023. Forensic Recovery Analysis of Lost Raid 0 Configuration on Network Attached Storage As Evidence in Court. *Jurnal Teknik Informatika (Jutif)*, *4*(4), 867–873. https://doi.org/10.52436/1.jutif.2023.4.4.1212

Prathivi, R., & Vydia, V. 2017. Analisa Pendeteksian Worm Dan Trojan Pada Jaringan Internet Universitas Semarang Menggunakan Metode Kalsifikasi Pada Data Mining C45 Dan Bayesian Network. *Jurnal Transformatika*, *14*(2), 77-81. http://dx.doi.org/10.26623/transformatika.v14i2.440

Putri, A. W. O. K., Aditya, A. R. M., Musthofa, D. L., & Widodo, P. 2022. Serangan hacking tools sebagai ancaman siber dalam sistem pertahanan negara (studi kasus: predator). *Global Political Studies Journal*, *6*(1), 35-46. http://ojs.unikom.ac.id/index.php/gps/article/view/6698

Rahmah, Elva. 2018. Akses dan Layanan Perpustakaan : Teori dan Aplikasi (Edisi Pertama). Jakarta : Prenamedia Group.

Ramdhani, A., Ramdhani, M. A., & Amin, A. S. 2014. Writing a Literature Review Research Paper: A step-by-step approach. *International Journal of Basic and Applied Science*, *03*(01), 47–56.

Rathee, S., & Garza-reyes, J. A. 2020. *An MCDA cause-effect factors model for the implementation of Greenstone Digital Library software*. *58*(11), 2543–2564. https://doi.org/10.1108/MD-09-2019-1268

Rauf, A., Idy, M. Y., Suryani, S., & Hardi, H. 2022. Tindak Pidana Penipuan Dalam Transaksi Jual Beli Secara Online. *In SISITI: Seminar Ilmiah Sistem Informasi dan Teknologi Informasi*. *11*(1), 8-18). https://www.ejurnal.dipanegara.ac.id/index.php/sisiti/article/view/937

Samad, A. N. 2014. Analisis Instrumen Cyber Terorrism Dalam Kerangka Sistim Hukum Internasional. *Jurnal Lex Crimen* , *7*(1), 1-101. https://www.academia.edu/download/45577469/SKRIPSI_LENGKAP-HI-_ALFIRA_NURLILIANI_SAMAD.pdf

Sari, I. 2023. Perbedaan Bentuk Kejahatan Yang Dikategorikan Sebagai Cyber Crime Dan Cyber Warfare. *JSI (Jurnal Sistem Informasi) Universitas Suryadarma* , *10* (1), 241-260.

Sayekti, Retno & Mardianto. 2019. *Perpustakaan Digital* : *Mengukur Penerimaan Inovasi Teknologi*. Medan : Perdana Publishing.

Situmorang, S., Lubis, H., & Manullang, J. 2022. Analysis Of Malware Methods Using Dynamic Analysis In Detecting Malware. *Jurnal Mantik*, *6*(2), 2639–2644.

Tjahjadi, E. V., & Santoso, B. 2023. Klasifikasi Malware Menggunakan Teknik Machine Learning. *Jurnal Ilmiah Ilmu Komputer*, *2*(1), 60–70.

Triandari, A. P. 2022. Studi Kepustakaan: Keamanan Informasi Di Perpustakaan Digital. *VISI PUSTAKA: Buletin Jaringan Informasi Antar Perpustakaan*, *24*(3), 237-250.https://doi.org/10.37014/visipustaka.v24i3.3175VISI

Umar, R., Riadi, I., & Kusuma, S. 2021. Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method. *IJID (International Journal on Informatics for Development)*, *10*(1), 53–61. https://doi.org/10.14421/ijid.2021.2423

Unyil, S. P. 2018. PENGEMBANGAN LITERACY KEISLAMAN DAN KEMELAYUAN BERBASIS DIGITAL DI STAIN SULTAN ABDURRAHMAN KEPULAUAN RIAU MENUJU ERA REVOLUSI INDUSTRI 4.0. *TREN PERPUSTAKAAN DI ERA MILLENIAL*, *93*, 99-122. http://repository.ukwms.ac.id/20172/1/Buku%20Prosiding%20Slimscomeetup%202018%20UKWMS.pdf#page=99

Utomo, T. P. 2021. Implementasi Teknologi Blockchain Di Perpustakaan: Peluang, Tantangan Dan

Hambatan. *Buletin Perpustakaan*, *4*(2), 173-200. https://journal.uii.ac.id/Buletin-Perpustakaan/article/view/22232

Widiyawati, A. T. 2019. Kajian Literasi Media Perpustakaan Digital Universitas Brawijaya (Studi Kasus pada Mahasiswa Tuna Netra Universitas Brawijaya). *Tik Ilmeu: Jurnal r*

Winata, A. P. 2019. Kejahatan Dunia Maya Bidang Akademik. *Media Pustakawan*, *26*(4), 303-310. https://doi.org/10.37014/medpus.v26i4.575

Wulandari, N. E. R., & Nugroho, E. 2017. E-learning: implikasinya terhadap pelayanan perpustakaan perguruan tinggi dan peran pustakawan. *Berkala Ilmu Perpustakaan Dan Informasi*, *13*(1), 87-96. https://doi.org/10.22146/bip.26199

Zulham. 2017. Penerapan Teknologi Informasi Menentukan Keberhasilan Dunia Perusahaan Industri. *Jurnal Warta*, *53*(9), 1689–1699.