ISSN 1411-2256 (Cetak) e-ISSN 2685-7138
DOI: https://doi.org/10.37014/visipustaka.v24i3.3175 VISI PUSTAKA, Vol. 24 No. 3 Desember 2022

STUDI KEPUSTAKAAN: KEAMANAN INFORMASI DI PERPUSTAKAAN DIGITAL

Asyifa Putri Triandari
Program Studi Perpustakaan dan Sains Informasi, Universitas Padjadjaran, Sumedang, Indonesia
asyifa21001@mail.unpad.ac.id

Diajukan : 22-07-2022 Direview : 18-10-2022 Direvisi : 24-10-2022 Diterima : 26-10-2022

ABSTRAK

Apakah semua informasi yang disimpan dalam perpustakaan digital, baik informasi berupa koleksi atau pun data diri pengguna benar-benar terjamin keamanannya? Penulisan artikel ilmiah ini membahas ancaman keamanan informasi di perpustakaan digital serta pencegahannya. Penelitian ini menggunakan metode kualitatif dengan teknik studi kepustakaan (*literature review*), yaitu teknik penelitian yang mengacu pada penelitian-penelitian terdahulu, beberapa pendapat para ahli, serta sumber-sumber tepercaya lainnya yang diperoleh penulis dengan mengkaji hasil penelitian-penelitian tersebut secara digital. Penelitian ini menunjukkan bahwa ancaman keamanan informasi pada perpustakaan digital tidak hanya menyerang program atau aplikasi yang digunakan untuk mengelola informasi saja, namun juga fisik benda untuk menyimpan informasi tersebut. Contoh ancaman keamanan informasi pada perpustakaan digital adalah *malware* yang terdiri dari berbagai jenis. Cara paling mudah agar suatu informasi yang disimpan tetap aman adalah dengan *back up* (membuat atau menggandakan suatu informasi). Namun, *back up* saja tidak cukup. Perlu adanya peningkatan kinerja pustakawan atau pun pihak pengelola lainnya dengan diikutkan berbagai pelatihan, baik yang diadakan nasional maupun luar negeri. Tak hanya SDM-nya saja, namun berbagai perangkat yang digunakan di dalam perpustakaan digital pun perlu diperbarui (*update*) agar sistem yang dijalankan tidak mudah mengalami gangguan. Selain itu, perpustakaan digital hendaknya dalam beberapa waktu sekali mengadakan simulasi kebobolan informasi, agar saat insiden yang tidak diharapkan tersebut terjadi, perpustakaan dapat mengambil langkah tepat agar dampak yang terjadi tidak semakin meluas.

Kata Kunci: Perpustakaan digital, keamanan informasi, pencegahan

ABSTRACT

Are all the information stored in digital libraries, both information in the form of collections or user personal data, guaranteed security? This article discusses the threats to information security in digital libraries and their prevention. This study uses a qualitative method with a research library technique, namely research that refers to previous studies, several expert opinions, and other reliable sources obtained by the author by digitally reviewing the research results. The research conducted shows that information security threats in digital libraries do not attack programs or applications that are used to manage information only, but also physical objects to store the information. Examples of information security threats to digital libraries are malware which consists of various types. The easiest way to keep information that is stored safely is by backing up (duplicating information). However, backup alone is not enough. It is necessary to improve the performance of librarians or other training managers by including various national and international events. Not only human resources, but various devices used in digital libraries also need to be updated so that the system that is run is not easily disturbed. In addition, digital libraries should in some time hold simulations of conceding information, so that when such unexpected incidents occur, libraries can take appropriate steps so that the impact that occurs is not more widespread.

Keywords: *Digital library, information security, their prevention*

PENDAHULUAN

Perpustakaan, yang berkaitan erat dengan koleksi buku atau informasi yang diletakkan di rak-rak buku, kini telah berkembang pesat dengan memanfaatkan peran teknologi. Telah banyak perpustakaan yang mengubah koleksi tercetaknya ke dalam format digital. Tidak hanya pihak perpustakaan saja yang dibuat mudah, namun para pengguna pun juga dimudahkan karena tidak harus berkunjung ke perpustakaan secara fisik.

Di Indonesia sendiri, telah ada beberapa perpustakaan yang berbentuk digital, meski sebenarnya kurang tepat pula penyebutan tersebut dikarenakan perpustakaan di Indonesia tidak ada yang benar-benar murni sebagai perpustakaan digital, melainkan masih dipadukan dengan perpustakaan konvensional. Terlepas dari penyebutan "perpustakaan digital" di Indonesia tepat atau tidak, setidaknya terdapat lebih dari lima perpustakaan di Indonesia yang sudah atau pernah berbasis digital. Perpustakaan tersebut antara lain Indonesia Digital Library Network (IDLN) yang diluncurkan pada Juni 2001 yang sayangnya saat ini sudah tidak dapat diakses kembali, *Spektra Virtual Library* (SVL) yang dibentuk pada tahun 1996, namun saat penulis mencoba masuk ke alamat *website,* ternyata laman tidak ditemukan, serta Garba Rujukan Digital Indonesia (GARUDA) yang saat ini masih dapat diakses melalui https://garuda.kemdikbud.go.id (Wulandari 2012) . Terdapat pula beberapa perpustakaan digital yang dapat diunduh dan diakses melalui aplikasi, seperti iPusnas, iJakarta, iKaltim, PustakaGita, dan Ruang Buku Kominfo.

Seperti contoh di atas, perpustakaan digital pasti berkaitan dengan penggunaan teknologi. Teknologi sendiri memiliki arti pengetahuan ilmiah yang digunakan untuk mengefektifkan cara dalam melakukan sesuatu, seperti penciptaan mesin atau suatu perangkat untuk memudahkan suatu pekerjaan (Hadadi 2017).

Rivalina dan Anwas pernah melakukan sebuah pengamatan terkait peran Teknologi Informasi dan Komunikasi (TIK) dibidang perpustakaan. Hasil penelitian tersebut menunjukkan dengan adanya TIK di perpustakaan, khususnya perpustakaan dengan basis digital, kebutuhan berbagai informasi seperti teks, audio, video, dan multimedia dapat diperoleh dengan mudah melalui internet. Selain itu, layanan yang diberikan oleh perpustakaan pun semakin cepat dan meluas dikarenakan pustakawan lebih mudah mengelola bahan pustaka dan menjadikan profesi ini lebih profesional.

Namun, peranan TIK khususnya di perpustakaan digital pun memiliki kekurangan, yaitu lemahnya sistem keamanan informasi yang dapat mengakibatkan terjadinya pencurian data, mutilasi data, *hacking* (pengaksesan suatu informasi secara tidak sah), *joy computing* (penggunaan komputer tanpa izin), *data diddling* (mengubah data valid menjadi tidak valid), dan lain-lain yang semua itu adalah ancaman, baik untuk pengguna maupun perpustakaan itu sendiri (Ali 2012) . Untuk mengatasi hal ini, diperlukan adanya pencegahan dan penanganan untuk meminimalisir risiko yang akan terjadi.

Penelitian yang dilakukan ini memiliki kesamaan dan perbedaan dengan penelitian-penelitian terdahulu. Kesamaan penelitian ini dengan penelitian-penelitian terdahulu adalah pembahasan mengenai ancaman keamanan informasi yang ternyata sudah menjadi keresahan sejak informasi-informasi tercetak dalam suatu lembaga berubah bentuk menjadi format digital. Sedangkan perbedaannya adalah setelah dilakukan pengkajian dari berbagai literatur, penulis menyarankan penelitian selanjutnya membahas mengenai ancaman serta pencegahan keamanan perpustakaan digital yang lebih spesifik, contohnya dengan mengadakan penelitian di perpustakaan digital tertentu, seperti di perpustakaan digital Ruang Buku Kominfo atau perpustakaan digital lainnya yang melihat dari sudut pandang keamanan informasi saja.

Penelitian ini membahas 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.

TINJAUAN PUSTAKA

1. Perpustakaan Digital

Menurut (Anday, et al., 2012), perpustakaan digital memiliki peran yang sangat penting dan merupakan posisi sentral dalam sebuah sistem. Perpustakaan digital sendiri adalah sebuah frasa yang terdiri dari dua kata, yaitu "perpustakaan" dan "digital" yang masing-masing kata tersebut memiliki arti yang berbeda.

Basuki (n.d) dalam modulnya yang berjudul Ilmu Pengantar Perpustakaan mendefinisikan perpustakaan adalah tempat yang berkaitan dengan buku. Menurut Undang-Undang Nomor 43 Tahun 2007 Pasal 1 ayat (1), perpustakaan adalah institusi pengelola koleksi karya tulis, karya cetak, dan/atau karya rekam secara profesional dengan sistem yang baku guna memenuhi kebutuhan pendidikan, penelitian, pelestarian, informasi, dan rekreasi para pemustaka. Sedangkan dalam Kamus Besar Bahasa Indonesia (KBBI), kata "perpustakaan" memiliki dua makna, yaitu: 1) tempat, gedung, ruang yang disediakan untuk pemeliharaan dan penggunaan koleksi buku dan sebagainya; 2) koleksi buku, majalah, dan bahan kepustakaan lain yang disimpan untuk dibaca, dipelajari, dibicarakan.

Dari ketiga pengertian di atas, dapat disimpulkan perpustakaan adalah sebuah institusi penghimpun koleksi karya tercetak maupun tidak tercetak yang dikelola secara profesional untuk memenuhi kebutuhan informasi masyarakat.

Beralih ke digital, kata digital memiliki makna merekam atau menyimpan informasi sebagai serangkaian angka 1 dan 0, untuk menunjukkan keberadaan sinyal (Cambridge Dictionary 2021) . Kata digital sendiri berasal dari Yunani, yaitu *digitus* yang artinya jari-jemari. Umumnya, manusia memiliki jari-jari di tangan kanan dan kiri, masing-masing terdapat lima jari, yang apabila dijumlahkan, menjadi 10. Angka 10 sendiri, terdiri dari dua angka, yaitu angka 1 dan 0. Kedua angka ini biasa disebut dengan bilangan *binary digit* (Syafnidawaty, 2020). Sedangkan dalam KBBI, kata digital memiliki makna sesuatu yang berhubungan dengan angka-angka untuk sistem perhitungan tertentu.

(Aji 2016) membagi digital menjadi dua arti. Yang pertama adalah definisi kata digital itu sendiri dan yang kedua adalah teori digital. Ia mendefinisikan digital sebagai suatu metode pokok yang rumit dan fleksibel untuk dijalankan dalam kehidupan manusia. Sedangkan teori digital adalah sebuah konsep yang awalnya segala sesuatu dilakukan secara manual kini dapat dilakukan secara otomatis, yang awalnya rumit menjadi ringkas.

Dari beberapa pengertian di atas yang mendefinisikan arti digital, dapat ditarik kesimpulan bahwa digital adalah sebuah cara untuk memudahkan kehidupan manusia agar lebih ter-otomatisasi melalui angka-angka yang membentuk perhitungan tertentu.

Apabila kata digital ini digabungkan dengan pembahasan sebelumnya, yaitu mengenai perpustakaan, maka jadilah frasa perpustakaan digital. Dari beberapa konsep yang telah dijabarkan, dapat diperoleh kesimpulan bahwa perpustakaan digital adalah institusi yang menghimpun koleksi dalam suatu format tertentu yang dikelola secara profesional dengan menggunakan sistem otomatisasi melalui perhitungan tertentu untuk memenuhi kebutuhan informasi masyarakat dengan cepat. Atau dapat pula diartikan dengan definisi yang lebih sederhana, yaitu suatu lembaga yang menyimpan dan mengelola informasi dengan memanfaatkan perangkat teknologi dalam lingkup virtual (bukan secara fisik).

2. Keamanan Informasi

Pada dasarnya, keamanan informasi adalah tindakan pencegahan dari akses, penggunaan, gangguan, pengungkapan, perekaman, inspeksi, modifikasi atau perusakan informasi yang dilakukan secara tidak sah, yang tujuan utamanya ialah memastikan suatu informasi yang disimpan tidak disalahgunakan (GeeksforGeeks 2021) . Keamanan informasi ini tidak hanya diterapkan untuk

informasi non digital saja, namun informasi berbasis digital pun juga hendaknya diterapkan sistem keamanan informasi. Hal ini seperti yang disampaikan Kurniawan (2018) yang mendefinisikan keamanan informasi sebagai penjagaan terhadap informasi dan data berupa fasilitas baik komputer atau pun non komputer yang disalahgunakan oleh pihak yang tidak berwenang.

Bagi perusahaan atau pun instansi, keamanan informasi tidak hanya digunakan sebagai cara untuk menjaga suatu informasi tetap aman, namun juga cara bagi sebuah perusahaan agar tetap berfungsi apabila informasi perusahaan tersebut mengalami kebobolan (Kurniawan 2018).

Secara umum, terdapat tiga aspek yang harus dipenuhi dari keamanan informasi, yaitu:

1. *Confidentiality* (kerahasiaan), yaitu sebuah informasi hanya dapat diakses oleh orang-orang yang memiliki wewenang
2. *Integrity* (integritas), yaitu sebuah informasi tidak dapat diubah oleh siapa pun yang tidak memiliki wewenang
3. *Availability* (ketersediaan), yaitu sebuah informasi harus tersedia saat dibutuhkan (BSN 2014).

Dari tiga aspek tersebut, Geeks for Geeks (2021) menambahkan tiga aspek yang berbeda mengenai keamanan informasi, sehingga total aspek tersebut berjumlah enam. Tiga aspek tambahan tersebut adalah *non-repudiation* (ketidakdapatan untuk menyangkal, yaitu satu pihak tidak dapat menolak untuk menerima pesan), *authenticity* (keaslian, yaitu setiap informasi yang diberikan berasal dari sumber terpercaya), dan *accountability* (yaitu apabila suatu informasi terdapat permintaan perubahan, maka harus ada persetujuan dari otoritas yang lebih tinggi).

(Fang, et al. 2020) menjelaskan *non-repudiation* dengan pengertian yang lebih detail, yaitu pelaku tidak dapat menyangkal transaksi (informasi) yang dilakukannya. Tujuan dari *non-repudiation* ini adalah untuk menghimpun, memelihara, menyimpan, serta menguji bukti yang tidak bisa dibantah mengenai informasi yang dikirim pelaku ke penerima. Terkait *confidentiality* (kerahasiaan), Pendit dalam jurnal yang dituliskan Wahdah (2020) mengungkapkan, kerahasiaan dalam dunia digital juga dapat diartikan sebagai pembatasan akses konten kepada pengguna dengan tujuan untuk menghindari pembajakan atau penjiplakan. Contoh pembatasan akses ini adalah pengguna hanya bisa membaca abstrak/sinopsis dari suatu konten. Bila pengguna dapat membaca keseluruhan isi konten, maka konten tersebut dibuat tidak dapat diunduh atau disalin (*copy paste*).

Setiap informasi memiliki nilai yang berbeda bagi suatu komunitas. Suatu komunitas bisa saja menganggap penting suatu informasi, sedangkan komunitas lainnya beranggapan biasa saja. Namun, apa pun tingkat kepentingan informasi tersebut, pengelola informasi akan menganggapnya penting karena kehilangan suatu informasi dapat menimbulkan masalah yang cukup rumit atau bahkan berbahaya bagi suatu komunitas. Apabila keseluruhan aspek keamanan informasi tersebut dapat terpenuhi, maka sumber daya informasi pun akan terjaga dari pihak-pihak yang tidak bertanggungjawab (BPPTIK 2014).

Di Indonesia sendiri, sebenarnya telah ada penelitian yang membahas keamanan informasi di perpustakaan tertentu yang berbasis aplikasi, yaitu iPusnas. Namun, pembahasan mengenai keamanan informasi dari penelitian tersebut hanya dilihat dari sudut pandang kerahasiaan, integritas, dan ketersediaan saja. Hasil penelitian yang dilakukan Galih (2020), menunjukkan bahwa dari segi kerahasiaan, iPusnas telah memiliki *licency policy* (kebijakan lisensi) yang artinya dapat dipercaya dan dapat dipertanggungjawabkan. Dari segi integritas, iPusnas membuat beberapa perjanjian dengan pengguna saat pembuatan akun, dan dari segi ketersediaan, judul yang tersedia sudah berjumlah ribuan. Meski begitu, jumlah eksemplar masing-masing judul tidaklah terlalu banyak dan masih terdapat judul-

judul buku fiksi populer yang tidak dapat ditemukan.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian kualitatif dengan teknik studi kepustakaan (*literature review*), yaitu teknik penelitian yang mengacu pada penelitian-penelitian terdahulu, beberapa pendapat para ahli, serta sumber-sumber terpercaya lainnya yang diperoleh penulis dengan mengkaji hasil penelitian-penelitian tersebut secara digital tanpa tinjauan langsung ke lapangan. *Literature review* dapat pula diartikan sebagai pemaparan mengenai teori, temuan, dan atau bahan penelitian yang telah dilakukan sebelumnya untuk dijadikan acuan atau dasar dari penelitian yang akan dilakukan (Syafnidawaty, Literature Riview 2020).

Penelitian yang menggunakan metode ini sebenarnya bisa saja hanya menuliskan hasil penelitian-penelitian yang sebelumnya telah dilakukan. Namun, pada umumnya, pemaparan penelitian yang menggunakan metode ini tetap menuliskan pola penelitian yang dilakukan serta menggabungkan ringkasan dan sintesis (Ramdhani, et al. 2014). Tujuan dari penelitian yang menggunakan metode *literature review* sendiri adalah agar peneliti mengetahui kontribusi keilmuan pada topik atau isu yang akan diteliti (Syafnidawaty, Literature Riview 2020) . Dengan menerapkan metode *literature review* pada penelitian ini, penulis berharap dapat lebih memahami permasalahan keamanan informasi pada perpustakaan digital.

Dalam menentukan bahan literatur yang akan dijadikan referensi pada artikel ini, penulis menerapkan model literasi *Empowering 8*, yaitu model literasi yang digunakan sebagai pendekatan menyelesaikan masalah dalam proses pembelajaran yang dikembangkan oleh IFLA pada tahun 2004 dan 2005. Model literasi ini mencakup proses *identify* (mengidentifikasi topik yang akan dibahas), *explore* (menggali lebih dalam informasi dari topik yang akan dibahas), *select* (memilih informasi yang sesuai dengan bahasan topik), *organizing* (mengorganisir informasi-informasi yang telah dihimpun), *create* (dari informasi yang telah dikumpulkan tersebut, dibuatlah kesimpulan menggunakan bahasa sendiri), *present* (mempersiapkan informasi yang telah dikumpulkan untuk dibagikan kepada orang lain, dalam hal ini penulisan artikel), *access* (menerima umpan balik dari orang lain, baik dari editor maupun dari pembaca), dan langkah terakhir yang dilakukan adalah *apply* (menggunakan umpan balik dari orang lain sebagai evaluasi langkah penelitian kedepannya) (Lisbdnetwork 2014).

HASIL DAN PEMBAHASAN

1. Sistem Keamanan Informasi di Perpustakaan Digital

Ajegbomogun dalam artikel yang ditulis oleh Erlianti (2017) memaknai sistem keamanan informasi di perpustakaan adalah “sistem yang dirancang untuk melindungi semua koleksi perpustakaan terhadap pihak-pihak lain yang tidak bertanggung jawab karena melakukan berbagai tindakan kejahatan seperti vandalisme bahkan pencurian terhadap koleksi perpustakaan”. Bila pemaknaan tersebut diimplementasikan pada perpustakaan digital, maka sistem keamanan informasi yang dimaksudkan haruslah dapat melindungi koleksi-koleksi digital yang disimpan oleh perpustakaan tersebut, baik yang disimpan dalam bentuk gambar dengan format *jpg., png.,* atau format lainnya maupun koleksi digital lainnya berupa audio atau teks yang format penyimpanan *file*-nya pun beragam.

Di Indonesia, pada 2020 lalu, Badan Standardisasi Nasional (BSN) mengenalkan SNI ISO/IEC 27001 sebagai Sistem Manajemen Keamanan Informasi (SMKI), yaitu suatu sistem yang digunakan untuk membuat, merasakan, melaksanakan memonitor, menganalisa, dan memelihara informasi yang dihimpun agar dapat menjaga, merahasiakan, serta merekam data privasi pengguna (BSN, 2014). SNI yang diperkenalkan ini adalah sistem keamanan informasi yang mengadopsi sistem keamanan yang telah diterbitkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC), yaitu

ISO/IEC 27001:2013 (Humas BSN 2020). Dari Laporan Kinerja Pusat Data dan Sistem Informasi (PUSDATIN), penerapan SNI ISO/IEC 27001:2013 ini dapat dikatakan berhasil. Ini terbukti dari penilaian tingkat kepatuhan yang mencapai nilai 100% dan sosialisasi mengenai SNI ISO/IEC 27001:2013 yang telah dilaksanakan oleh BSN di berbagai perguruan tinggi di Indonesia (BSN 2020).

Walau demikian, keamanan informasi yang paling utama adalah dari administrator atau pengelola informasi itu sendiri, dalam hal ini adalah pustakawan. Mereka yang memasang, mengelola dan menghubungkan jaringan haruslah orang-orang yang jujur. Pekerjaan administrator yang benar adalah mengatur jaringan dan sistem *file* agar dapat diakses sesuai oleh pengguna. Merekalah yang membuat kata sandi, memasang sistem pengaman, menjalankan program dan memahami seluk beluk permasalahan dalam jaringan. Mereka pula yang melakukan *backup* (mencadangkan) suatu informasi agar saat terjadi permasalahan terhadap suatu informasi, informasi yang dicadangkan tersebut dapat digunakan.

2. Ancaman Keamanan Perpustakaan Digital

Perubahan format penyimpanan informasi dari cetak ke noncetak di perpustakaan digital bukan hanya berupa koleksi umum saja, namun juga termasuk informasi personal dari *user* (pengguna/pemustaka). Alasannya adalah untuk dapat mengakses konten, pengguna diperlukan mengisi atau menunjukkan identitas diri (Fox and ElSherbiny 2011).

Pada perpustakaan digital, layanan yang diberikan dapat berupa mengumpulkan data identitas pengguna berupa lokasi, melacak penggunaan layanan perpustakaan, dan lain-lain. Dikutip dari *IFLA Statement on Privacy in the Library Environment*, (2015, hal. 1), Majelis Umum PBB pada tahun 2013 dan 2014 telah menyuarakan kebijakan terkait privasi untuk semua negara, yaitu menghormati dan melindungi hak privasi, termasuk dalam konteks komunikasi digital, yang pernyataan tersebut diadopsi dari resolusi mengenai *right to privacy in the digital age* (hak privasi di era digital). Karena itu, perpustakaan digital dapat memilih data pribadi apa yang dikumpulkan dari pengguna. Mereka dapat pula meminta penyedia layanan komersial untuk melindungi data privasi pengguna atau menolak layanan yang berlebihan bila hal tersebut dapat membahayakan privasi pengguna. Namun, peran perpustakaan mungkin saja terbatas untuk mendapatkan pengetahuan praktik pengumpulan data yang dilakukan oleh layanan komersial atau lembaga pemerintah dalam mengelola data privasi pengguna tersebut. Yang menjadi pertanyaan adalah apakah semua informasi di perpustakaan yang menggunakan teknologi internet, baik informasi berupa koleksi atau pun data diri pengguna benar-benar terjamin keamanannya?

Menurut (Arms 2000) , pada dasarnya, internet sendiri tidak aman. Justru internet yang paling banyak terjadi kejahatan. Orang dapat dengan mudah mengamati informasi yang datang dan pergi melalui jaringan. Server web dan surat elektronik adalah contoh program yang paling sering digunakan oleh perpustakaan digital dan merupakan program yang paling tidak aman.

Dikarenakan internet tidak aman, keamanan informasi paling sederhana bisa dimulai dari penggunaan komputer individu, yang secara fisik keamanan pada komputer individu dapat dilakukan dengan pembatasan akses terhadap komputer tersebut, misalnya dengan nama *login* dan kata sandi. Apabila komputer dapat diakses oleh banyak pengguna, maka diperlukan pihak yang dapat mengontrol untuk menambah atau mengurangi informasi (koleksi).

Namun, terkait penggunaan komputer ini, ancaman yang terjadi bisa dari internal maupun eksternal. Ancaman internal tidak hanya dari pustakawan saja, namun bisa dari mitra, konsultan, *vendor*, kontraktor, dan karyawan lainnya yang turut mengelola perpustakaan digital. Sedangkan contoh ancaman dari pihak

eksternal adalah pesaing perpustakaan digital dengan mengotak-atik sistem perpustakaan digital tersebut (Kurniawan 2018).

Menurut Zimerman dari jurnal yang ditulis oleh (Anday, Francese, Huurdeman, Yilmaz, & Zengenene, 2012), komputer yang digunakan untuk pengaturan di perpustakaan digital belum dapat disebut aman karena rawan terhadap sejumlah serangan sistem berupa virus atau dapat juga terjadi *cybercrime* (kejahatan dunia maya). Setidaknya terdapat lima kegiatan yang termasuk dalam *cybercrime,* di antaranya pencurian data, penggunaan komputer tanpa izin, pengaksesannya tidak sah, pengubahan data valid menjadi tidak valid, dan sabotase data yang diperlukan sehingga data menjadi rusak dan tidak dapat digunakan. Ali (2012) berpendapat, terdapat beberapa alasan seseorang melakukan tindak kejahatan dalam dunia maya yaitu untuk unjuk gigi saja atau bahkan kepentingan komersial. Apabila yang diincar adalah data pengguna, biasanya pelaku memiliki motif tersendiri, semisal untuk *marketing*.

Ancaman untuk komputer ini semakin sulit untuk diatasi dikarenakan pendistribusian informasi di perpustakaan digital menggunakan sistem jaringan komputer. Artinya, informasi tersebut diteruskan dari satu komputer ke komputer lainnya. Jika pengelolaan akses hanya ada di komputer pusat, maka akses dapat efektif diatur secara lokal. Namun, apabila komputer pusat sebagai repositori mengalami masalah, maka semua informasi yang tersimpan di semua komputer pun juga akan turut bermasalah (Arms 2000) . Repositori sendiri memiliki arti tempat penyimpanan beragam aplikasi atau program yang telah diolah agar bisa diakses melalui internet (Syafnidawaty, 2020).

Beragam program yang telah disimpan di dalam komputer pun dapat mengalami serangan terhadap sistem contohnya seperti *malware* yang mencakup virus*, Trojan horse*, *worms, awareness, spyware*, *pornware, keystroke loggers*, pencurian kata sandi, dan lain-lain (Zimerman 2009).

Malicious software atau yang biasa disebut *malware* adalah istilah yang digunakan untuk *software* (perangkat lunak) yang merusak sistem di komputer. Berdasarkan tujuan pembuatannya, (Gustifa 2017) mengkategorikan *malware* menjadi tiga kelompok. Kelompok pertama adalah *malware* yang bertujuan menginfeksi program di komputer, terdiri dari virus dan *worm*.

Virus dalam bidang teknologi informasi memiliki arti suatu program yang dapat memperbanyak diri untuk menyerang program di komputer (Namanya, Cullen, et al. 2018). Selain menyerang program komputer, virus juga dapat mencuri informasi, membuat iklan, bahkan mencuri uang untuk kejahatan.

Seperti virus, *worm* adalah suatu program yang dapat melipatgandakan diri untuk menyerang program komputer. Yang membedakan *worm* dengan virus adalah cara penyebarannya. Bila virus membutuhkan bantuan manusia untuk memperbanyak diri, maka *worm* dapat melakukannya secara mandiri (Namanya, Cullen, et al. 2018).

Kelompok *malware* yang kedua adalah *malware* yang tujuannya bernaung atau bersembunyi di komputer. *Malware* jenis ini meliputi *Trojan horse* dan *backdoor*. *Trojan horse* atau biasa disebut *trojan* adalah sebuah perangkat lunak yang legal untuk diunduh. Dikarenakan legal, tentu seharusnya tidak ada masalah. Yang menjadi masalah adalah seringkali *trojan* yang diunduh ini juga membawa virus, yang akhirnya dapat memberikan akses kepada penyerang melalui jarak jauh (Namanya, Cullen, et al. 2018). Sedangkan *backdoor* atau pintu jebakan adalah suatu program yang dapat memblokir sistem pengamanan di komputer sehingga penyerang dapat masuk ke program komputer tanpa perlu melalui sistem pengamanan pada umumnya (Ali, 2012).

Kelompok *malware* yang ketiga adalah *malware* yang bertujuan untuk mencuri manfaat atau keuntungan dari suatu program komputer, contohnya adalah *spyware, adware, bot, root kit,* dan *ransomware*.

Sesuai kata dasarnya *"spy"* memiliki arti memata-matai. Definisi lengkapnya, *spyware* adalah suatu program yang berfungsi mengamati aktivitas komputer yang diserang kemudian mengirim informasi tersebut kepada penyerang, dan terkadang memiliki fungsi tambahan yaitu mengganggu jaringan internet dan merusak sistem pengamanan komputer (Namanya, Cullen, et al. 2018).

Adware yang merupakan singkatan dari *Ad software*, adalah suatu program yang memiliki tujuan menampilkan layanan iklan *pop up* di perangkat lunak (Namanya, Cullen, et al. 2018). Meski *adware* tidak mengambil uang yang kita miliki, namun *adware* adalah bisnis yang sangat menggiurkan bagi para pengiklan. Semakin banyak orang yang melihat iklan, maka semakin banyak pula penghasilan yang didapat (Kersh 2020) . *Adware* ini semakin berbahaya bagi komputer bila dikemas dengan *spyware* karena selain menampilkan iklan yang dirancang sebagai pendapatan bagi penyerang, juga dapat mencuri informasi dan mengamati aktivitas pengguna (Namanya, Cullen, et al. 2018).

Bot adalah kependekan dari *robot* yang maksudnya adalah suatu program yang dapat menjalankan suatu operasi tertentu di komputer. (Eslahi, Salleh and Anuar 2012) mengungkapkan bahwa *bot* dirancang untuk merusak target seperti komputer tanpa sepengetahuan pemilik target tersebut. *Malware bot* ini bisa saja digunakan secara sah, seperti penjawab pesan otomatis di *WhatsApp* atau pun *email*, pemrograman video, konten online, dan lain sebagainya (Namanya, Cullen, et al. 2018). Namun, *bot* ini juga bisa menjadi berbahaya karena dapat merusak jaringan suatu komputer, yang artinya, apabila terdapat satu komputer bermasalah dikarenakan *bot* ini, komputer lain yang terhubung dengan komputer tersebut pun juga akan mengalami masalah (Namanya, Cullen, et al. 2018).

Hampir mirip dengan *backdoor*, *rootkit* adalah *malware* yang berhubungan sistem pengamanan komputer. Bedanya adalah apabila cara kerja *backdoor* dengan memblokir sistem keamanan komputer, maka cara kerja *rootkit* adalah dengan membuat sistem keamanan komputer tidak mendeteksi adanya gangguan program. Menurut (Liu, et al. 2012), *rootkit* adalah perangkat lunak atau kode yang digunakan untuk menyembunyikan berkas-berkas, registry, modul kode, dan lain-lain. Tujuan utamanya adalah agar pengguna tidak dapat mengidentifikasi aktivitas penyerang (Najoan 2020) . *Root kit* ini termasuk *malware* yang sangat berbahaya karena dapat mengambil alih penuh suatu sistem. Karena cara kerja *root kit* sangat efektif, penghapusan dari komputer sangat bergantung cara manual (Namanya, Cullen, et al. 2018). Yang artinya, cara paling ampuh untuk mengatasi *root kit* adalah dengan dilakukan oleh manusia, bukan dengan sistem otomatisasi.

Ransomware adalah suatu program yang merusak komputer dengan mengunci akses berkas dari pengguna, yang apabila pengguna tersebut hendak mengakses kembali berkas yang dikunci, maka pengguna harus melakukan transaksi ke alamat yang diminta (Namanya, Cullen, et al. 2018). "Biasanya, *file* yang menjadi target *ransomware* adalah berkas dengan format .doc, .txt, .ppt, .jpeg, .zip, .pdf, .cgi, . mdb, .db1, .db, .dbx, .rft, .dsw, .cbm, .cpp, . asm, .gzip, .key, dan .pgp" (Luo & Liao dalam Imaji, 2019) Permasalahan yang paling serius adalah pembayaran yang telah dilakukan belum tentu menjamin pengembalian *file* dan belum tentu pula dapat menghapus *ransomware* dari sistem (Imaji 2019).

Tentang *ransomware*, telah ada kasus nyata yang menyerang perpustakaan digital dengan *malware* jenis ini. Pada 2017 lalu, terjadi peretasan terhadap 700 komputer di Perpustakaan Umum St. Louis, Amerika Serikat. Untuk membuka server yang diretas, Perpustakaan Umum St. Louis diminta untuk menyerahkan sejumlah *bitcoin* kepada peretas yang ditolak oleh perpustakaan tersebut dikarenakan menurut penyelidikan FBI, mata uang *bitcoin* adalah mata uang *online* yang sulit ditelusuri keberadaannya. Alhasil, solusi yang dilakukan perpustakaan tersebut

adalah menghapus keseluruhan sistem komputer yang kemudian harus dibuat ulang dengan memakan waktu yang tidak sebentar (Kean 2017).

Karena informasi mengenai data diri pengguna ataupun keuangan tidak disimpan di dalam server, informasi tersebut dinyatakan aman. Meski demikian, kasus ini menunjukkan bahwa perpustakaan digital rentan terhadap peretasan. Keahlian mengoperasikan sistem komputer serta selalu memperbarui sistem adalah upaya yang dapat ditempuh oleh pustakawan untuk mengatasi *ransomware ini*.

Ancaman keamanan informasi berikutnya adalah *phishing* yang berasal dari kata *fishing* yang artinya memancing. *Phishing* ini dapat dimaknai sebagai upaya yang dilakukan seseorang untuk "memancing" orang lain memberikan data pribadinya secara sukarela tanpa disadari oleh pemilik data pribadi tersebut (Pangaribuan 2022).

Hingga tahun 2022 ini, data dari laman resmi Kementerian Keuangan Republik Indonesia mengungkapkan bahwa ancaman keamanan informasi yang paling sering terjadi di tahun 2022 ini adalah *ransomware, phishing,* dan mata uang kripto.

3. Pencegahan Ancaman Keamanan Informasi

Untuk mencegah kehilangan data, *backup* atau membuat cadangan suatu informasi adalah cara yang paling sering digunakan oleh instansi atau lembaga (Anday, et al., 2012). Namun, *backup* saja tidak cukup. Menurut Fetscherin & Schmid dalam jurnal yang ditulis oleh (Fox and ElSherbiny 2011), terdapat beberapa cara untuk melindungi informasi dalam sebuah teknologi, yaitu:

- *Encryption* (enkripsi)
- Penggunaan kata sandi
- Pemindaian sidik jari
- *Watermarking*
- Tanda tangan digital
- *Copy detection system*
- Sistem pembayaran

Encryption adalah istilah yang berasal dari Bahasa Yunani, yaitu *kryptos* yang artinya adalah tersembunyi. Menurut Olufohunsi (2019), *encryption* atau yang dalam Bahasa Indonesia disebut enkripsi adalah proses merubah bentuk pesan yang awalnya berbentuk *plaintext* (pesan yang dapat dimengerti manusia) menjadi *ciphertext* (pesan yang tidak dimengerti manusia) dengan menggunakan algoritma enkripsi (Bassel). Untuk mengubah pesan ke bentuk awal (*plaintext*), diperlukan sebuah kunci (*key*) yang hanya dimiliki oleh pihak yang sah. Yang artinya, bila terdapat pihak lain yang ingin melihat isi pesan tersebut, namun tidak memiliki kunci yang dimaksud, makai @ tidak akan bisa mengakses pesan tersebut. Contoh enkripsi ini di kehidupan nyata adalah penggunaan kata sandi (*password)* komputer, ATM, dan *e-commerce* (Rashad 2016).

Penggunaan kata sandi dapat pula menjadi cara untuk mencegah kehilangan informasi. Namun, penggunaan kata sandi ini justru yang paling sering menjadi objek penyerangan oleh *hacker*. Para *hacker* yang sudah ahli, dapat dengan mudah menemukan kata sandi dengan menebak informasi pengguna atau mencari tahu kebiasaan pengguna (Hatzivasilis 2020) . Menurutnya, terdapat beberapa pola kata sandi yang sebaiknya dihindari untuk menjaga informasi, diantaranya yaitu:

1. Kata-kata dengan angka tambahan yang sederhana (misal: dina123, alfin45, jodi08)
2. Kata-kata dengan simbol sederhana (misal: alvi@an, n@gaterb@ang, p@assw0rd)
3. Kata atau karakter yang berulang (misal: sansan, aaabbbccc, 232323)
4. Informasi pribadi yang berkaitan dengan pengguna (misal: tanggal lahir, nama pasangan, daerah tempat tinggal), serta masih banyak lagi pola-pola serupa yang sebaiknya dihindari dalam penggunaan kata sandi

Selain penggunaan kata sandi, cara lain yang dapat dilakukan dengan tujuan serupa adalah dengan pemindaian sidik jari.

Bila *encryption* dan kata sandi bertujuan agar pihak lain tidak mengetahui isi pesan, *watermarking* memiliki tujuan berbeda, yaitu untuk menjaga keaslian isi pesan. Menurut T. B Cahyana dan Danang Jaya dalam Solichin (2010), *watermarking* adalah teknik menyisipkan data ke dalam elemen multimedia seperti foto, video, atau musik. Data yang disisipkan tersebut harus dapat dideteksi oleh multimedia yang dimasukinya. Teknik menyisipkan data ini, terdiri dari beragam macam teknik dan teknik yang paling sering digunakan adalah *image watermarking*, yaitu data yang disisipkan bertujuan melindungi gambar asli Contoh sederhana dari *watermarking* ini adalah saat kita mengunduh sebuah foto dari internet, terdapat tulisan atau logo yang mengidentitaskan pemilik foto tersebut. (Solichin, 2010).

Sama halnya dengan *watermarking*, penggunaan tanda tangan digital juga berfungsi untuk menjaga keaslian dan keautentikan sebuah informasi. Dengan adanya tanda tangan digital, dapat dilakukan pembuktian atau verifikasi untuk mengetahui informasi yang diterima telah dimodifikasi atau tidak (Sulaiman, Ihwani and Rizki n.d.). Dengan tanda tangan pula, dokumen yang terbukti dimodifikasi akan dengan mudah untuk diminta pertanggungjawaban.

Beda lagi halnya dengan *copy detection system*. Tujuan dari *copy detection system* ini adalah agar tidak terjadi penjiplakan atau peniruan atas karya seseorang/lembaga. Dengan adanya *copy detection* ini, akan sangat mudah melacak plagiarisme yang dilakukan oleh seseorang, baik plagiat foto, video, gambar, tulisan, dan sebagainya. Menurut (Hien and Nguyen 2015) , tindakan plagiarisme adalah masalah serius, baik dalam dunia penerbitan ilmiah maupun dalam ranah pendidikan. Pada umumnya, *copy detection system* sangat bagus menilai dan menemukan keidentikkan suatu konten. Namun, sistem keamanan informasi ini memiliki kekurangan, yaitu sistem ini tidak memberi tahu banyak mengenai perubahan yang terjadi pada salinannya. Selain itu, apabila konten salinan berubah secara total, algoritma pada sistem ini dapat gagal memulihkan parameter transformasi yang tepat (Allili, Casemajor and Talbi 2019).

Selain cara melindungi informasi yang telah disebutkan di atas, terdapat cara lain yang dapat dilakukan, yaitu dengan diberlakukannya sistem pembayaran. Sistem pembayaran ini, sepintas mungkin terlihat sama dengan *ransomware*. Padahal, dua hal tersebut sebenarnya sangat jauh berbeda, terutama dalam hal kepemilikan dan cara kerjanya. Seperti yang dijelaskan pada paragraf-paragraf sebelumnya, *ransomware* adalah penguncian akses informasi dari pengguna, yang bila pengguna ingin mendapatkan akses kembali, pengguna harus membayar sejumlah uang yang diminta. Dapat dilihat, sebenarnya kepemilikan informasi berada di tangan pengguna. Namun, ada pihak lain yang mengunci akses informasi tersebut dengan harapan pengguna membayar tebusan. Bisa saja pihak yang melakukan penguncian akses sama sekali tidak menaruh minat dengan informasi yang ia ambil, namun bisa juga pihak tersebut sangat mengincar informasi pengguna. Meski pengguna melakukan pembayaran, hal itu tidak menjamin pengembalian akses.

Lain halnya dengan sistem pembayaran. Pada sistem pembayaran, pengguna belum memiliki informasi yang diinginkan atau yang diperlukannya. Dan agar pengguna memiliki informasi tersebut, pengguna membayar sesuai ketentuan dari pemilik informasi tersebut. Di sini, pembayaran sifatnya adalah sebagai jaminan. Yang artinya, bila pembayaran telah dilangsungkan, maka pengguna dapat mengakses informasi yang diinginkannya. Bila ternyata pengguna belum memperoleh akses, maka pengguna dapat mengajukan klaim kepada lembaga atau perusahaan yang merupakan pemilik informasi tersebut.

Dari tujuh cara yang dijelaskan sebelumnya, Ali (2012) memberi tiga saran tambahan untuk mencegah terjadinya ancaman terhadap informasi, yaitu 1) meningkatkan profesionalisme

pustakawan dengan diikutkan berbagai kursus mengenai keamanan data; 2) selalu memperbarui dan meningkatkan sarana prasarana, baik *hardware* ataupun *software;* dan 3) senantiasa membuat *file* cadangan secara teratur.

Terkait profesionalisme seorang pustakawan di era digital, (Safitri 2017) mengungkapkan terdapat empat belas *skills* (kemampuan) yang diperlukan untuk menguasai perangkat teknologi informasi. Empat belas kemampuan tersebut antara lain:

a. Menguasai desain *database* dan manajemen *database*
b. Menguasai data *warehousing*
c. Memahami proses penerbitan elektronik
d. Menguasai perangkat keras
e. Menguasai arsitektur informasi
f. Memahami sumber informasi elektronik
g. Integrasi informasi
h. Menguasai desain *intranet* dan *ekstranet*
i. Menguasai aplikasi *software* (perangkat lunak)
j. Menguasai pemrograman
k. *Workflow* (alur kerja)
l. Memahami pemrosesan teks
m. Menguasai metadata
n. Menguasai manajemen informasi melalui perangkat lunak

IFLA (2021) pun dalam laman blognya menyebutkan 10 aspek yang perlu dilakukan oleh pustakawan perpustakaan digital untuk meningkatkan keprofesionalitasnya, yang lima diantaranya berfokus membahas terkait keamanan informasi. Salah satunya adalah aspek *check your cybersecurity*. Pada aspek ini, dijelaskan bahwa pustakawan perpustakaan digital hendaknya mengenkripsi informasi yang dikirim secara *online*, selalu memastikan bahwa perangkat komputer yang digunakan selalu di-*update*, menggandakan informasi-informasi yang telah dihimpun, membuat kata sandi yang kuat, meninjau ulang aset-aset yang dimiliki serta membuat prediksi risiko yang akan dihadapi, mempertimbangkan vendor mana saja yang dapat mengakses data pengguna, serta tentunya lebih proaktif dalam mengintegrasikan keamanan informasi.

Meski segala cara telah dilakukan untuk menjaga informasi agar tetap aman, terkadang masih ada kejadian yang tidak diinginkan, seperti kebocoran informasi. Lantas, tindakan apa yang perlu dilakukan bila keamanan informasi mengalami kebobolan? (Dhillon 2017) menuliskan enam tahapan yang seharusnya selalu dilatih oleh suatu lembaga untuk mengantisipasi kebobolan keamanan informasi. Enam tahapan tersebut yaitu:

1. Menilai kerusakan yang terjadi
2. Mencoba membatasi kerusakan agar tidak menyebar, salah satunya dengan memblokir jaringan sistem
3. Rekam jejak kejadian secara tertulis, perihal yang dituliskan meliputi akun yang disusupi, sistem yang terpengaruh, layanan yang terhambat, data dan jaringan yang terdampak, serta jumlah dan jenis kerusakan yang terjadi
4. Libatkan penegak hukum
5. Apabila insiden yang terjadi membahayakan informasi individu, mereka perlu diberitahukan
6. Belajar dari insiden agar tidak terulang lagi di masa depan

KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa keamanan informasi perpustakaan digital belum sepenuhnya aman. Terdapat banyak ancaman yang dapat membuat informasi yang dihimpun rusak atau bahkan hilang. Pada tahun 2022 ini, ancaman keamanan informasi yang perlu mendapat perhatian khusus adalah *ransomware, phishing,* dan mata uang kripto. Untuk mencegah dan mengatasi hal tersebut, SDM yang mengelola perpustakaan digital diharapkan dapat meningkatkan profesionalismenya dengan diikutsertakan berbagai pelatihan, seperti pelatihan penggunaan komputer, penggunaan *software*, kursus bahasa pemrograman, dan penggandaan informasi, baik yang diadakan di dalam maupun di luar negeri. Tak hanya itu,

pustakawan perpustakaan digital pun hendaknya selalu aktif dalam meninjau semua aset yang dimiliki serta membuat prediksi terkait risiko kemungkinan yang terjadi di masa yang akan datang. Namun, bukan hanya SDM-nya saja yang ditingkatkan kinerjanya, berbagai perangkat yang digunakan di dalam perpustakaan digital pun perlu di-*update* (diperbarui) agar sistem yang dijalankan tidak ketinggalan dengan sistem yang digunakan oleh *hacker* (peretas). Di Indonesia, perpustakaan yang telah berbasis digital dapat menggunakan SNI ISO/IEC 27001 sebagai sistem keamanan informasi di perpustakaan tersebut. Selain itu, perpustakaan digital hendaknya dalam beberapa waktu sekali mengadakan simulasi kebobolan informasi, agar saat insiden yang tidak diharapkan tersebut terjadi, perpustakaan dapat mengambil langkah tepat agar dampak yang terjadi tidak semakin meluas. Penelitian yang perlu dilakukan selanjutnya adalah pembahasan mengenai ancaman serta manajemen keamanan informasi di perpustakaan digital yang lebih spesifik, contohnya keamanan informasi di perpustakaan digital Ruang Buku Kominfo atau dapat pula di perpustakaan digital lainnya.

DAFTAR PUSTAKA

Aji, R. 2016. "Digitalisasi Era Tantangan Media (Analisis Kritis Kesiapan Fakultas Dakwah dan Komunikasi Menyongsong Era Digital)." *Islamic Communication Journal.*

Ali, I. 2012. "Kejahatan Terhadap Informasi (Cybercrime) dalam Konteks Perpustakaan Digital." April. Accessed December 18, 2021. https://www.perpusnas.go.id/magazine-detail.php?lang=id&id=8217.

Allili, M.S., N. Casemajor, and A. Talbi. 2019. "Image Copy Detection and Evolution Visualisation Using Three Graphs."

Anday, A., E. Francese, H. C. Huurdeman, M. Yilmaz, and D. Zengenene. 2012. "Information Security Issues in a Digital Library Environment: A Literature Review." 117-137.

Arms, W. Y. 2000. "Access Management and Security." *In Digital Library* (MIT Press). Accessed December 23, 2021. https://www.cs.cornell.edu/wya/DigLib/text/Chapter7.html.

Badan Pengembangan Bahasa. 2016. "Digital." Accessed December 2021. https://kbbi.kemdikbud.go.id/entri/digital.

—. 2016. *Perpustakaan.* Accessed December 2021. https://kbbi.kemdikbud.go.id/entri/perpustakaan.

Basuki, S. n.d. "Ilmu Pengantar Perpustakaan."

BPPTIK. 2014. "Keamanan Informasi." *Artikel*, March. Accessed December 20, 2021. https://bpptik.kominfo.go.id/2014/03/24/404/keamanan-informasi/.

BSN. 2020. "Laporan Kinerja Pusat Data dan Sitem Informasi (PUSDATIN)." Accessed April 8, 2022. https://bsn.go.id/uploads/download/laporan_kinerja_2020_ess_ii_pusdatin_-_final_13012021.pdf.

—. 2014. "Teknologi Informasi - Teknik Keamanan - Sistem Manajemen Keamanan Informasi - Gambaran Umum dan Kosakata."

Cambridge Dictionary. 2021. *Digital.* Accessed December 2021. https://dictionary.cambridge.org/dictionary/english/digital.

Dhillon, G. 2017. "What to do Before and After a Cybersecurity Breach?" Accessed April 10, 2022. https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf.

Erlianti, Gustina. 2017. "Penerapan Sistem Keamanan Koleksi pada Perpustakaan Kota Yogyakarta." *Shaut al-Maktabah* 9 (1): 115-124. Accessed November 15, 2022. https://rjfahuinib.org/index.php/shaut/article/view/110/76.

Eslahi, M., R. Salleh, and N. B. Anuar. 2012. "Bots and Botnets: An Overview of Characteristics, Detection, and Challenges." *IEEE International Conference of Control System, Computing, and Engineeriing.* Penang: ResearchGate. Accessed April 6, 2022. https://www.researchgate.net/publication/261087741_Bots_and_botnets_An_overview_of_characteristics_detection_and_challenges.

Fang, Weidong, Wei Chen, Wuxiong Zhang, Jun Pei, Weiwei Gao, and Guohui Wang. 2020. "Digital Signature Scheme for Information Non-repudiation in Blockchain: A state of the art review." *EURASIP Journal on Wireless Communications and Networking.* Accessed April 9, 2022. https://d-nb.info/1210812738/34.

Fox, Edward, and N. ElSherbiny. 2011. "Security and Digital Libraries." April: 151-158. Accessed December 2021. doi:10.5772/15762.

Galih, Aulia Puspaning. 2020. "Keamanan Informasi (Information Security) pada Aplikasi Perpustakaan iPusnas." June. Accessed April 11, 2022. https://www.researchgate.net/publication/343285496_Keamanan_Informasi_Information_Security_Pada_Aplikasi_Perpustakaan_IPusnas.

GeeksforGeeks. 2021. *What is Information Security.* Oct 31. Accessed December 20, 2021. https://www.geeksforgeeks.org/what-is-information-security/.

—. 2021. *What is Information Security?* October 31. Accessed December 19, 2021. https://www.geeksforgeeks.org/what-is-information-security/.

Gustifa, R. 2017. "Malware." April. Accessed December 23, 2021. http://edocs.ilkom.unsri.ac.id/1312/1/MALWARE%20-%2009011281320007.pdf.

Hadadi, Al. 2017. "Pengertian Teknologi serta Definisi Teknologi Menurut Para Ahli." July. Accessed December 17, 2021. https://www.scribd.com/document/354570483/Pengertian-Teknologi-Serta-Definisi-Teknologi-Menurut-Para-Ahli.

Hatzivasilis, G. 2020. "Password Management: How Secure Is Your Login Process." *Model-driven Simulation and Training Environments for Cybersecurity (MSTEC 2020)* (ResearchGate). Accessed April 10, 2022. https://www.researchgate.net/publication/346538020_Password_Management_How_Secure_Is_Your_Login_Process.

Hien, N. L., and T. O. Nguyen. 2015. "A Copy Detector Method Based on SCAM and PPCHECKER." *the Sixth International Symposium* (ResearchGate). Accessed April 10, 2022. https://www.researchgate.net/publication/301455375_A_Copy_Detection_Method_Based_on_SCAM_and_PPCHECKER.

Humas BSN. 2020. "BSN Dukung PPATK dalam Penerapan SNI ISO/IEC 27001:2013 ." Accessed April 7, 2022. https://bsn.go.id/main/berita/detail/11183/bsn-dukung-ppatk-dalam-penerapan-sni-isoiec-270012013.

IFLA. 2015. "Statement on Privacy in the Library Environment." (International Federation of Library Associations and Institutions) 1-2. Accessed December 22, 2022. https://www.ifla.org/wp-content/uploads/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf.

—. 2021. *The 10-Minute Digital Librarian #8: Chech Your Cybersecurity.* July 21. Accessed November 18, 2022. https://blogs.ifla.org/lpa/2021/07/21/the-10-minute-digital-librarian-8-check-your-cybersecurity/.

Imaji, Asibi. 2019. "Ransomware Attacks: Critical Analysis, Threats, and Prevention Methods." (ResearchGate). Accessed April 7, 2022. https://www.researchgate.net/publication/332551447_Ransomware_Attacks_Critical_Analysis_Threats_and_Prevention_methods.

Kean, Danuta. 2017. *Ransomware Attack Paralysis St Louis Libraries as Hackers Demand Bitcoins.* The Guardian. Accessed April 8, 2022. https://www.theguardian.com/books/2017/jan/23/ransomware-attack-paralyses-st-louis-libraries-as-hackers-demand-bitcoins.

Kersh, N. 2020. "Adware." Accessed April 6, 2022. https://www.allot.com/resources/TB_Adware.pdf.

Kurniawan, Kresna Pradiva. 2018. "Pengertian Keamanan Informasi." November. Accessed December 20, 2021. https://www.researchgate.net/publication/329237876_Pengertian_Keamanan_Informasi.

Lisbdnetwork. 2014. *IFLA Empowering 8 Model of Information Literacy.* December 23. Accessed November 18, 2022. https://www.lisedunetwork.com/ifla-empowering-8-model-of-information/.

Liu, Leian, Zuanxing Yin, Haitao Lin, and Yuli Shen. 2012. "Research and Design of Rootkit Detection Method." *2012 International Conference on Medical Physics and Biomedical Engineering.* ResearchGate. 852-857. Accessed April 7, 2022. doi:10.1016/j.phpro.2012.05.145.

Najoan, Xaverius. 2020. "Analisis Aspek Keamanan dalam Menghadapi Rootkit Berbasis Mesin Virtual (VMBR)." Accessed December 23, 2021. https://media.neliti.com/media/publications/141536-ID-analisis-aspek-keamanan-dalam-menghadapi.pdf.

Namanya, Anitta Patience, Andrea J. Cullen, Irfan Awan, and Jules Pagna Diss. 2018.

"The Worldof Malware: An Overview." *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud).* Barcelona: ResearchGate. Accessed December 23, 2021. doi:10.1109/FiCloud.2018.00067.

Olufohunsi, Temitope. 2019. "Data Encryption." (ResearchGate). Accessed April 9, 2022. https://www.researchgate.net/publication/337889039_DATA_ENCRYPTION_Olufohunsi_T#:~:text=Encryption%20is%20the%20process%20of,algorithm%20(Bassel).

Pangaribuan, Edgar Joseph Ronny. 2022. *Keamanan Informasi dan Tren Serangan Tahun 2022.* June 29. Accessed November 19, 2022. https://www.djkn.kemenkeu.go.id/kpknl-medan/baca-artikel/15179/Keamanan-Informasi-dan-Tren-Serangan-Tahun-2022.html.

Ramdhani, Abdullah, Muhammad Ali Ramdhani, and Abdusy Syakur Amin. 2014. "Writing a Literature Review Research Paper: A step-by-step approach." *International Journal of Basics and Applied Sciences* (Insan Akademika Publications). Accessed May 26, 2022. https://www.researchgate.net/publication/311735510_Writing_a_Literature_Review_Research_Paper_A_step-by-step_approach.

Rashad, A. F. 2016. "Contoh Kasus Kriptografi di Kehidupan Nyata yang Terjadi pada Tahun 2014/2015." Accessed April 9, 2022. http://edocs.ilkom.unsri.ac.id/86/1/Contoh%20Kasus%20Kriptografi%20di%20Kehidupan%20Nyata%20yang%20Terjadi%20Pada%20Tahun%202014.pdf.

Rivalina, Rahmi, and Oos M. Anwas. 2013. "Teknologi Informasi dan Komunikasi dalam Optimalisasi Peprustakaan." *Jurnal Teknodik* 17. Accessed December 17, 2021. https://jurnalteknodik.kemdikbud.go.id/index.php/jurnalteknodik/article/view/81/81.

Safitri, Tiara Hilda. 2017. "Pustakawan Profesional di Era Digital." *Jurnal Kepustakwanan dan Masyarakat Membaca* 33. Accessed December 2021. https://ejournal.unsri.ac.id/index.php/jkdmm/article/view/JKDMMV33No2%3B059-066/pdf.

Solichin, Achmad. 2010. "Digital Watermarking untuk Melindungi Informasi Multimedia." (ResearchGate). Accessed April 10, 2022. https://www.researchgate.net/publication/236885804_Digital_Watermarking_untuk_Melindungi_Informasi_Multimedia.

Sulaiman, Oris Krianto, Mohamad Ihwani, and Salman Fajar Rizki. n.d. "Model Keamanan Informasi Berbasis Tanda Tangan Digital dengan Data Encryption Standard (DES) Algorithm." *Jurnal Nasional Informatika dan Tekologi Jaringan* 1: 14-19. Accessed April 10, 2022. doi:10.30743/infotekjar.v1i1.82.

Syafnidawaty. 2020. *Apa Itu Repository?* Universitas Raharja. November. Accessed December 23, 2021. https://raharja.ac.id/2020/11/13/apa-itu-repository/.

—. 2020. "Digital." May. Accessed December 19, 2021. https://raharja.ac.id/2020/05/14/digital/.

—. 2020. *Literature Riview.* Universitas Raharja. October. Accessed May 26, 2022. https://raharja.ac.id/2020/10/13/literature-review/.

UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 43 TAHUN 2007 TENTANG PERPUSTAKAAN. 2007. November. Accessed December 19, 2021. https://peraturan.bpk.go.id/Home/Details/39968/uu-no-43-tahun-2007.

Wahdah, Siti. 2020. "Perpustakaan Digital, Koleksi Digital dan Undang-Undang Hak Cipta." *Pustaka Karya: Jurnal Ilmiah Ilmu Perpustakaan dan Informasi* 8: 26-36.

Wulandari, Dian. 2012. "Jaringan Perpustakaan Digital di Indonesia: Hambatan dan Wacana Pengembangannya." April. Accessed April 7, 2022. https://www.perpusnas.go.id/magazine-detail.php?lang=en&id=8221#:~:text=Jaringan%20perpustakaan%20digital%20di%20Indonesia%20telah%20berkembang%20sejak%20tahun%202000,GARUDA%20(Garba%20Rujukan%20Digital).

Zimerman, Martin. 2009. "Protect Your Library's Computers." *emerald.* doi:10.1108/03074801011044070.