PENERAPAN KEYCLOAK UNTUK AUTENTIKASI DAN OTORISASI PADA ARSITEKTUR MICROSERVICE

Skripsi

oleh:

YABES QINEN YEHDEYA
71180350

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2024

PENERAPAN KEYCLOAK UNTUK AUTENTIKASI DAN OTORISASI PADA ARSITEKTUR MICROSERVICE

Skripsi

Diajukan kepada Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

YABES QINEN YEHDEYA
71180350

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2024

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

PENERAPAN KEYCLOAK UNTUK AUTENTIKASI DAN OTORISASI PADA ARSITEKTUR MICROSERVICE

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi mana pun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 01 Februari 2024

MATE

YABES QINEN YEHDEYA
71180350

HALAMAN PERSETUJUAN

Judul Skripsi	:	PENERAPAN KEYCLOAK UNTUK AUTENTIKASI DAN OTORISASI PADA ARSITEKTUR MICROSERVICE
Nama Mahasiswa	:	YABES QINEN YEHDEYA
NIM	:	71180350
Mata Kuliah	:	Skripsi (Tugas Akhir)
Kode	:	TI0366
Semester	:	Genap/Ganjil
Tahun Akademik	:	2023/2024

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 15 Februari 2024

Dosen Pembimbing I	Dosen Pembimbing II
Yuan Lukito, S.Kom., M.Cs	Budi Susanto, S.Kon., M.T.

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI/TESIS/DISERTASI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Kristen Duta Wacana, saya yang bertanda tangan di bawah ini:

Nama	: Yabes Qinen Yehdeya
NIM	: 71180350
Program studi	: Informatika
Fakultas	: Teknologi Informasi
Jenis Karya	: Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Kristen Duta Wacana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

"PENERAPAN KEYCLOAK UNTUK AUTENTIKASI DAN OTORISASI PADA ARSITEKTUR MICROSERVICE"

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti/Noneksklusif ini Universitas Kristen Duta Wacana berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama kami sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Yogyakarta
Pada Tanggal : 07 JUNI 2024

Yang menyatakan

(Yabes Qinen Yehdeya)
NIM.71180350

HALAMAN PENGESAHAN

PENERAPAN KEYCLOAK UNTUK AUTENTIKASI DAN OTORISASI PADA ARSITEKTUR MICROSERVICE

Oleh: YABES QINEN YEHDEYA / 71180350

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
pada tanggal 15 Februari 2024

Yogyakarta, 15 Februari 2024
Mengesahkan,

Dewan Penguji:

1. Yuan Lukito, S.Kom., M.Cs ----------
2. Budi Susanto, S.Kom., M.T. ----------
3. Matahari Bhakti Nendya, S.Kom., M.T. ----------
4. Maria Nila Anggia Rini, S.T, M.T.I ----------

Dekan

(Restyandito,S.Kom.,MSIS.,Ph.D.)

Ketua Program Studi

(Joko Purwadi, S.Kom., M.Kom)

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS SECARA ONLINE UNIVERSITAS KRISTEN DUTA WACANA YOGYAKARTA

Saya yang bertanda tangan di bawah ini:

NIM	:	71180350
Nama	:	Yabes Qinen Yehdeya
Prodi / Fakultas	:	Teknologi Informasi / Informatika
Judul Tugas Akhir	:	Penerapan Keycloak untuk Autentikasi dan Otorisasi pada Arsitektur Microservice

bersedia menyerahkan Tugas Akhir kepada Universitas melalui Perpustakaan untuk keperluan akademis dan memberikan **Hak Bebas Royalti Non Ekslusif** (*Non-exclusive Royalty-free Right*) serta bersedia Tugas Akhirnya dipublikasikan secara online dan dapat diakses secara lengkap (*full access*).

Dengan Hak Bebas Royalti Nonekslusif ini Perpustakaan Universitas Kristen Duta Wacana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk *database*, merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenar-benarnya.

Yogyakarta, 01 Februari 2024

Yang menyatakan,

(71180350 – Yabes Qinen Yehdeya)

KATA PENGANTAR

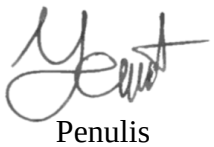
Segala puji dan syukur kepada Tuhan yang maha kasih, karena atas segala rahmat, bimbingan, dan bantuan-Nya maka akhirnya Skripsi dengan judul "PENERAPAN KEYCLOAK UNTUK SAUTENTIKASI DAN OTORISASI PADA ARSITEKTUR MICROSERVICE" ini telah selesai disusun.

Penulis memperoleh banyak bantuan dari kerja sama baik secara moral maupun spiritual dalam penulisan Skripsi ini, untuk itu tak lupa penulis ucapkan terima kasih yang sebesar-besarnya kepada:

1. Tuhan Yesus dan Roh Kudus yang tetap memberikan kesehatan dan kemampuan dalam menyertai dari awal proses belajar sebagai mahasiswa hingga akhir skripsi,
2. Orang tua yang selama ini telah sabar membimbing, mendoakan, dan memberikan semangat untuk penulis sampai akhir skripsi,
3. Restyandito, S.Kom, MSIS., Ph.D selaku Dekan FTI,
4. Joko Purwadi, S.Kom., M.Kom selaku Kaprodi Informatika,
5. Yuan Lukito, S.Kom., M.Cs selaku Dosen Pembimbing 1, yang telah memberikan ilmunya dan dengan penuh kesabaran membimbing penulis,
6. Budi Susanto, S.Kom., M.T. selaku Dosen Pembimbing 2 yang telah memberikan ilmu dan kesabaran dalam membimbing penulis,
7. Keluarga tercinta yang memberikan dukungan dengan semangat dan doa dalam pengerjaan skripsi,
8. Teman-teman seperjuangan yang masih memberikan motivasi dan semangat dalam mendorong penulis untuk mengerjakan skripsi hingga selesai,
9. Teman-teman dan para majelis Gereja Kristen Jawa memberikan dorongan untuk menyelesaikan skripsi,
10. Adel menjadi *support* sistem penulis dan tetap menemani penulis dari awal hingga proses skripsi selesai dan menjaga moral, spiritual motivasi untuk belajar selama ini.

Laporan proposal/skripsi ini tentunya tidak lepas dari segala kekurangan dan kelemahan, untuk itu segala kritikan dan saran yang bersifat membangun guna kesempurnaan skripsi ini sangat diharapkan. Semoga proposal/skripsi ini dapat bermanfaat bagi pembaca semua dan lebih khusus lagi bagi pengembangan ilmu komputer dan teknologi informasi.

Yogyakarta, 01 Februari 2024



Penulis

Yabes Qinen Yehdeya

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

PENERAPAN KEYCLOAK UNTUK AUTENTIKASI DAN OTORISASI PADA ARSITEKTUR MICROSERVICE

Oleh

YABES QINEN YEHDEYA
71180350

Sistem informasi rumah sakit merupakan salah satu media yang digunakan untuk memberikan informasi pelayanan dari rumah sakit kepada Masyarakat. Mengingat data pasien bersifat rahasia sehingga harus disimpan di *data base local* dan di Indonesia terdapat Undang-Undang yang membahas mengenai privasi dan data pribadi yaitu UU no 11 tahun 2008, dalam sistem layanan kesehatan rumah sakit memerlukan sistem keamanan yang dapat membatasi akses *user* ke *Application Programing Interface* (API).

Oleh karena itu, perlu dilakukan pengembangan sistem yang dapat memverifikasi dan memvalidasi *user* dalam mengakses data pada sistem. Diperlukan sistem *Auth service* yang dapat melakukan proses *Authentication* dan *Authorization* di setiap *service.*

Berdasarkan hasil test skenario wildcard endpoint yang di test menggunakan postman, penulis mendapatkan kesimpulan yaitu berhasil untuk menerapkan Authentication dan Authorization pada arsitektur sistem layanan multi klinik dengan keycloak. Autentikasi dan otorisasi yang diterapkan penulis dengan keycloak efektif dalam mengelola identitas, memastikan autentikasi yang aman, dan mengatur otoritas sesuai dengan hak akses serta peran masing-masing pengguna. Hal tersebut dapat dibuktikan dengan suksesnya pengujian dalam mengakses endpoint API menggunakan aplikasi postman sesuai dengan task skenario yang dibuat. Maka Maka, penelitan ini telah mencapai tujuan dari penulis yang ingin mengetahui efektifitas Authentication dan Authorization dalam pemberian role dan hak akses terhadap user dan dari REST API yang dibangun

dapat menjadi dasar dalam pengembangan sistem terintegrasi lebih lanjut. **Kata-kata kunci** : Authorization, Authentication, Keycloak

ABSTRACT

IMPLEMENTATION KEYCLOAK FOR AUTHENTICATION AND AUTHORIZATION IN MICROSERVICE ARCHITECTURE

By

YABES QINEN YEHDEYA

71180350

The hospital information system is one of the media used to provide information about hospital services to the public. Considering that patient data is confidential so it must be stored in a local database and in Indonesia there is a law that discusses privacy and personal data, namely Law No. 11 of 2008, in the health service system hospitals require a security system that can limit user access to the Application Programming Interface(API).

Therefore, it is necessary to develop a system that can verify and validate users in accessing data on the system. An Auth service system is required to carry out the Authentication and Authorization process for each service.

Based on the results of the wildcard endpoint test scenario which was tested using Postman, the author came to the conclusion that it was successful in implementing Authentication and Authorization in a multi-clinic service system architecture with Keycloak. The authentication and authorization implemented by the author with Keycloak is effective in managing identity, ensuring secure authentication, and setting authority according to the access rights and roles of each user. This can be proven by successful testing in accessing the API endpoint using the Postman application according to the task scenario created. So, this research has achieved the aim of the author who wanted to know the effectiveness of Authentication and Authorization in granting roles and access rights to users and the REST API that was built could become the basis for further integrated system development. **Keywords** : Authorization, Authentication, Keycloak

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Sistem informasi rumah sakit merupakan salah satu media yang digunakan untuk memberikan informasi pelayanan dari rumah sakit kepada Masyarakat. Rumah sakit merupakan sebuah organisasi yang melayani Masyarakat di bidang Kesehatan. Sebuah Lembaga sosial gereja yang bergerak pada bidang Kesehatan yaitu Yayasan Kristen untuk Kesehatan Umum (YAAKUM) kini memiliki rumah sakit yang terdapat di beberapa tempat seperti: Parakan, Purwokerto, Surakarta (Solo), Semarang, dan Yogyakarta. Rumah sakit yang berada di bawah Yayasan YAKKUM menjalan informasi secara mandiri tanpa melibatkan rumah sakit lainnya. Mengingat data pasien bersifat rahasia sehingga harus disimpan di *database local* dan di Indonesia terdapat Undang-Undang yang membahas mengenai privasi dan data pribadi yaitu UU no 11 tahun 2008, dalam sistem layanan kesehatan rumah sakit memerlukan sistem keamanan yang dapat membatasi *user* dalam akses ke *Application Programing Interface* (API). Oleh karena itu, perlu dilakukannya pengembangan sistem yang dapat memverifikasi dan memvalidasi *user* dalam mengakses data pada sistem.

Dalam pengembangan sistem informasi layanan kesehatan multi klinik, khususnya bagian *backend*, memerlukan *developing secure services* dalam memberikan hak akses kepada *user*. Dalam mengatasi pengembangan sistem tersebut, dibutuhkan arsitektur yang dapat mempermudah dalam pengerjaan sistem. Arsitektur *Microservices* salah satunya, yaitu dengan menerapkan aplikasi-aplikasi kecil atau *services* yang bersifat *independent* dan saling terhubung antar *servicenya*. Dengan implementasi arsitektur microservices, karena semua *services* diakses dari luar(internet), jika terjadi isu dalam *frame work,security bug*, atau terjadi kebocoran data maka di setiap *microservicesnya* harus benar-benar dijaga. Pada sistem multi klinik yang memberikan layanan berbasis digital, diperlukannya peran *security* pada sistem. API yang dibangun dengan *REST* API, memerlukan keamanan karena

memiliki data yang sensitif dan memiliki informasi yang hanya bisa di akses oleh *user* tertentu. Dengan penerapan *Authentication* dan *Authorization* dalam *REST* API, *user* akan diberikan has akses atau diberi batasan untuk mengakses *REST* API. Jika menggunakan *Authentication* dan *Authorization* maka harus diimplementasikan di semua *services* supaya tidak terjadi duplikasi proses. Diperlukan sistem *Auth service* yang dapat melakukan proses *Authentication* dan *Authorization* di setiap *service*. *Auth service* akan memvalidasi *request* yang masuk dari luar apakah data *user* sudah di-*verify* atau belum dan melihat apakah *user* tersebut memiliki *role* yang sesuai dengan yang sudah terdaftar pada sistem. Dengan begitu, proses *Authentication* dan *Authorization* perlu diterapkan dalam *microservices*.

Dalam penelitian ini, penulis hanya berfokus pada *Authentication* dan *Authorization* pada sistem. Proses *Authentication* dan *Authorization* akan dilakukan, jika proses *Auth* sukses maka *request* dan data *Auth* akan dikirimkan ke *service* yang diminta jika proses *Auth* gagal maka akan di *reject*. Penulis menggunakan *Keycloak* sebagai *identity provider* dalam *Authentication* dan *role-based Authorization* sebagai otorisasi yang digunakan *user* untuk mengakses ke API. *Authentication* dan *Authorization* dilakukan agar *user* dapat *login* ke sistem, setelah itu *user* akan mendapatkan *role user* masing-masing untuk mengakses *service* yang dibutuhkan tetapi tidak semua *service* bisa diakses oleh *user* hanya beberapa saja. Karena setiap *service* memiliki data atau informasi yang bersifat rahasia.

1.1 Rumusan Masalah

Berdasarkan penjelasan dari latar belakang di atas, maka rumusan masalah yang penulis dapatkan adalah untuk mengetahui efektivitas implementasi *Authentication* dan *Authorization* pada arsitektur *microservices* dalam memanajemen dan menangani akses ke sumber daya di sistem informasi layanan multi klinik.

1.2 Batasan Masalah

Penelitian ini dibatasi dengan hal-hal berikut:

1. Pengembangan sistem hanya sebatas *prototype*.
2. Pengembangan sistem dilakukan pada *service* yang berkaitan dengan autentikasi dan otorisasi.
3. Penerapan autentikasi dalam pengujian sistem menerapkan konfigurasi *granttype authorization code.*
4. Penerapan otoriasi diterapkan di setiap *service.*
5. Pengujian autentikasi dan otorisasi sangat bergantung pada registrasi pengguna yang bukan merupakan domain penelitan penulis.
6. Implementasi *endpoint* API hanya sebatas *mocking* yang berdasar dokumen API Design, sehingga tidak memperhatikan detail fungsionalitas API
7. Sistem yang dibangun dengan *framework Spring Boot* pemrograman *java*.
8. Data yang digunakan merupakan data *dummy*.

1.3 Tujuan Penelitian

Tujuan penelitian ini adalah menerapkan *Authentication* dan *Authorization* pada sistem dalam arsitektur *microservices* di mana diperlukannya *resource server* untuk menjaga sisi keamanan setiap *servicenya*.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini antara lain:

1. Menambah pengalaman dalam membuat aplikasi *prototype* dengan arsitektur *Microservices*.
2. Membangun sistem autentikasi dan otorisasi pada setiap *service*.
3. Penerapan *REST* API dalam memberikan akses pada setiap entitas *services* sistem.

1.5 Metodologi Penelitian

Penulis melakukan metode-metode sebagai langkah untuk melakukan penelitian dengan cara sebagai berikut:

1. Metode Studi Literatur

   Penulis melakukan studi literatur untuk mendapatkan informasi yang terkait dengan penelitian yang dilakukan, pencarian yang dapat dilakukan berupa buku, jurnal atau artikel, dan bahan studi literatur lainnya tentang *Authentication*, *Authorization*, keamanan API, *REST* API, dan *Microservice*.

2. Metode Pengembangan Sistem

   Pada tahap ini Penulis akan mengimplementasikan juga desain arsitektur sistem. Pada tahap ini penulis melakukan implementasi dan sekaligus mempelajari kebutuhan teknis dari arsitektur sistem berdasarkan data kebutuhan yang diperoleh dari proses sebelumnya. Kemudian melakukan implementasi *Authentication* dan *Authorization* pada sistem.

3. Metode Evaluasi

Pada tahap ini penulis melakukan evaluasi dengan melakukan pengujian terhadap sistem untuk mengetahui apakah sistem yang dibangun sudah berjalan dengan baik dan sesuai dengan kebutuhan.

1.6 Sistematika Penulisan

Sistematika penulisan merupakan penjelasan dari rangkaian bab yang sudah disusun, pada bab 1 berisi latar belakang, perumusan masalah, batasan masalah, tujuan penelitian. Bab 2 berisi tentang tinjauan pustaka yang diambil dari jurnal-jurnal penelitian yang judul dan topiknya sama dengan apa yang penulis teliti. Landasan teori yang menjelaskan tentang materi dan teori yang ada dalam penelitian. Bab 3 berisikan penjelasan tentang langkah penulis mengerjakan penelitian dan metode-metode yang digunakan penulis dalam mengerjakan penelitian. Bab 4 berisi mengenai pengerjaan dan hasil pengujian sistem pada aplikasi sistem. Bab 5 berisi kesimpulan dan saran dari penelitian yang sudah dilakukan oleh penulis.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil *test* skenario *wildcard endpoint* yang di *test* menggunakan *postman,* penulis mendapatkan kesimpulan yaitu berhasil untuk menerapkan *Authentication* dan *Authorization* pada arsitektur sistem dengan *keycloak. Autentikasi* dan otorisasi yang diterapkan penulis dengan *keycloak* efektif dalam mengelola identitas, memastikan autentikasi yang aman, dan mengatur otoritas sesuai dengan hak akses serta peran masing-masing pengguna. Hal tersebut dapat dibuktikan dengan suksesnya pengujian dalam mengakses *endpoin*t API menggunakan aplikasi *postman* sesuai dengan task skenario yang dibuat. Maka penelitian ini telah mencapai tujuan dari penulis yang ingin mengetahui efektivitas *Authentication* dan *Authorization* dalam pemberian *role* dan hak akses terhadap setiap *user* dan dari REST API yang dibangun dapat menjadi dasar dalam pengembangan sistem terintegrasi lebih lanjut.

5.2 Saran

Dari penelitian yang penulis lakukan, terdapat saran yang penulis berikan dalam membangun penelitian lebih lanjut. Sistem yang dibuat masih dalam bentuk *prototype* sistem yang merupakan salah satu sistem yang digunakan untuk registrasi pengunjung ke rumah sakit. API yang dibangun dapat digunakan sebagai dasar untuk pengembangan sistem terintegrasi selanjutnya baik berbasis web, *mobile* dan *dekstop.* Sehingga akan lebih baik jika penelitian dan pembuatan API yang sudah dilakukan dapat dikembangkan untuk nantinya dapat diterapkan di pengembangan sistem dengan lebih baik.

DAFTAR PUSTAKA

Alchuluq, L. M., & Nurzaman, F. (2021). ANALISIS PADA ARSITEKTUR MICROSERVICEUNTUK LAYANAN BISNIS TOKOONLINE. *TEKINFOVol.22*, 61-68.

Andress, J. (2011). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition.* Amsterdam: Syngress.

Aziz, A. S., & Safriatullah, S. (2021). Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius. *Journal of Informatics and Computer Science Vol.7*, 106-112.

Darmadi, E. A. (2018). PERANCANGAN SISTEM OTENTIKASI RADIUS PADA PENGGUNA JARINGAN WIRELESS UNTUK MENINGKATKAN KEAMANAN JARINGAN KOMPUTER. *IKRA-ITH INFORMATIKA Vol 2*, 9-16.

Divyabharathi, D., & Cholli, N. (2020). A Review on Identity and Access Management Server (KeyCloak). *International Journal of Electrical and Power Engineering*, 17-22.

Nair, V. (2019). *Practical Domain-Driven Design in Enterprise Java: Using Jakarta EE, Eclipse MicroProfile, Spring Boot, and the Axon Framework.* -: Apress.

Payara, G. R., & Tanone, R. (2018). Penerapan FirebaseRealtimeDatabase Pada PrototypeAplikasi Pemesanan Makanan Berbasis Android. *urnal Teknik Informatika dan Sistem Informasi*, 397-406.

Pradana, I. A. (2017, Febuari 03). *Mengenal Spring Boot*. Diambil kembali dari CODEPOLITAN: https://www.codepolitan.com/blog/spring-boot-pengenalan-588da0c4bedd1/

Ramadhani, A. R., Bhawiyuga, A., & Siregar, R. A. (2018). Implementasi Access Control List Berbasis Protokol MQTT pada Perangkat. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2824-2831.

Richardson, C. (2018). *Microservices Patterns: With examples in Java.* Shelter Island: Manning Publications.

Saputra, M. H., & Nabil, L. M. (2021). PENERAPAN ARSITEKTUR MICROSERVICE PADA SISTEM TATA KELOLA. *Jurnal Teknik Informatika*, 22-28.

Subandri, Hanadwiputra, S., & Prabowo, K. M. (2018). Optimalisasi Radius Server Sebagai Sistem Otentikasi dan Otorisasi untuk. *Jurnal PowerPlant, Vol. 6*, 86-92.

Waschke, M. (2017). *Personal Cybersecurity: How to Avoid and Recover from Cybercrime.* Washington: Apress.