



**Model *Attribute Based Access Control* (ABAC) Pada
Sistem Lemari Penyimpanan Bukti Digital (LPBD)**

Mohamad Fadli Panende, S.Kom

16917111

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Magister Teknik Informatika

Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

2018

Lembar Pengesahan Pembimbing

**Model Attribute Based Access Control (ABAC)
Pada Lemari Penyimpanan Bukti Digital (LPBD)**

Mohamad Fadli Panende, S.Kom

16917111



الجامعة الإسلامية
الاندونيسية
Pembimbing

A handwritten signature in blue ink, appearing to be 'Dr. Imam Riadi', is written over a horizontal line. The signature is fluid and cursive.

Dr. Imam Riadi, M.Kom

Lembar Pengesahan Penguji

**Model Attribute Based Access Control (ABAC)
Pada Lemari Penyimpanan Bukti Digital (LPBD)**

Mohamad Fadli Panende, S.Kom

16917111

ISLAM

Yogyakarta, April, 2018

Tim Penguji,

Dr. Imam Riadi, M.Kom

Ketua

Yudi Prayudi, S.Si., M.Kom

Anggota I

Dr. Bambang Sugiantoro, M.T

Anggota II

Mengetahui,

Ketua Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST., M.Sc.

Abstrak

Model Attribute Based Access Control (ABAC) Pada Lemari Penyimpanan Bukti Digital (LPBD)

Faktor penting dalam proses investigasi sebuah kasus *cybercrime* yaitu hal yang terkait dengan barang bukti yang ditemukan. Bukti elektronik maupun bukti digital yang ditemukan dalam sebuah kasus kejahatan harus tetap terjaga keasliannya untuk dapat dipertanggung jawabkan dipengadilan. Sistem lemari penyimpanan bukti digital (LPBD) menjadi salah satu solusi untuk permasalahan manajemen bukti digital ini yang berdasar pada *digital evidence cabinet* (DEC), hanya saja sistem tersebut belum dilengkapi dengan model akses kontrol yang baik. Sistem LPBD seharusnya dibuat tidak hanya berdasar pada permasalahan-permasalahan tentang manajemen bukti digital saja, akan tetapi komponen-komponen penting lainnya dalam lemari penyimpanan bukti digital itu sendiri yaitu pengaturan aksesnya, sehingga skema atau desain akses kontrol *policy* terhadap LPBD menjadi sangat penting. Akses kontrol yang digunakan terhadap LPBD sebelumnya dibuat hanya dengan mekanisme autentikasi dan authorisasi *user* saja, tidak adanya parameter lain yang lebih kompleks untuk mendukung sebuah permintaan akses yang dilakukan pada sistem LPBD. Penelitian ini dilakukan pada LPBD dengan tahapan yang dimulai dari melakukan identifikasi masalah, studi literature, pembuatan konsep ABAC, implementasi, simulasi dan skenario kasus, melakukan pengujian, hasil dan analisa, serta memberikan kesimpulan. Adapun tujuan dilakukannya penelitian ini yaitu membangun rancangan akses kontrol pada LPBD menggunakan pendekatan *attribute based access control* (ABAC) dan melakukan pengujian terhadap keamanan sistem LPBD dalam segi pemberian hak akses pada *user*. Berdasarkan hasil pengujian yang dilakukan menggunakan *tools* khusus untuk menguji kinerja akses kontrol, didapatkan hasil bahwa rancangan ABAC yang dibangun dapat berjalan dengan baik sebagaimana mestinya yang diharapkan. Pendekatan menggunakan ABAC ini dapat dijadikan solusi atas permasalahan akses kontrol LPBD sebelumnya, khususnya dalam proses identifikasi user. Penggunaan pendekatan ABAC pada LPBD ini disebabkan ABAC merupakan model akses kontrol *policy* yang lebih fleksibel dalam penerapan atribut terhadap *user*, dan *hierarchy* XACML yang dapat mendukung kebutuhan-kebutuhan akses kontrol yang digunakan pada LPBD.

Kata kunci

Access Control, ABAC, LPBD, XACML, DEC

Abstract

Attribute Based Access Control (ABAC) Model on The Digital Evidence Cabinet System (DECS)

An important factor of the investigation process of a cybercrime case is related to the evidence found. Electronic evidence and digital evidence found in a criminal case must be kept authentic in order to be accountable in court. Digital evidence storage cabinet system (DESC) is one solution to overcome this digital evidence management based on digital cabinet evidence (DEC), It's just that the system is not equipped with good access control model. The DESC system should be built not only on the issues of digital proof management alone, will the other important components in the digital proof storage cabinet itself are the access arrangement, so the scheme or the design of the access control policy on the DESC becomes very important. The access controls used on previous DESCs were created only with user authentication and authorization mechanisms, in the absence of more complex parameters to support a request made on the DESC system. This research was conducted on LPBD with stages starting from identifying research problem, literature study, ABAC concept, implementation, simulation and scenario, testing, result and analysis, and giving conclusion. This additional purpose uses access control on the DESC using to attribute based access control (ABAC) approaches and conducts tests of the security of DESC systems in the size of user permissions. Based on the results of tests conducted using a special tool for access control operations, obtained results are eligible ABAC built can run well as expected. By using ABAC this can be used as a solution to access access control DESC before, especially in the process of user identification. The use of the ABAC approaches to the DESC is due to ABAC being a more flexible model of access control policy of the application of attributes to users, and the XACML hierarchy that can support the access controls needs used DESC.

Keywords

Access Control, ABAC, DESC, XACML, DEC

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, April 2018

Mohamad Fadli Panende, S.Kom



Daftar Publikasi

Tidak Ada Publikasi Bagian Dari Thesis Ini

Halaman Kontribusi

Tidak Ada Kontribusi Pihak Lain

Halaman Persembahan

Segala puji bagi ALLAH SWT yang tidak pernah berhenti memberikan pertolongan maha pengasih maha penyayang, serta salawat bagi Rasulullah SAW rahmat bagi semesta alam.

Kupersembahkan karyaku kepada kedua orang tua, keluarga sanak saudara yang selalu kurindukan selama masa studi ini berlangsung, melalui ini juga penulis menghaturkan permohonan maaf yang sebesar-besarnya kepada keluarga yang selalu aku repotkan.

Kepada almarhum ayahanda Drs. Moh. Ramli Panende, M.Si yang telah berpulang kerahmatullah ketika penulis sedang menempuh studi pascasarjana di Yogyakarta, melalui ini juga penulis bersembah sujud memohon ampun atas kesalahan yang pernah penulis lakukan kepada almarhum semasa hidupnya dan tidak sempat melihat hembusan nafas terakhir almarhum ayahanda. Penulis sangat menyangi ayahanda.

Kepada Almarum kakek HI. Usman Panende, BA yang telah mendidik dan membesarkan penulis hingga SMA, dan nenekda Dra HJ. Dinar Maloto yang penulis tinggalkan untuk melanjutkan studi dan juga berperan penting dalam mendidik dan membesarkan penulis hingga sekarang, tak henti-hentinya penulis mengucapkan banyak terima kasih.

Semua penulis terpaksa lakukan untuk masa depan penulis

Semua penulis lakukan untuk membangun keluarga

Kata Pengantar

Assalamualaikum Wr. Wb.

Alhamdulillah hirobbi 'alamin penulis ucapkan kepada ALLAH SWT yang selalu memberikan kesehatan dan keselamatan pada diri penulis untuk menyelesaikan tesis ini dengan judul **“Model Attribute Based Access Control (ABAC) Pada Lemari Penyimpanan Bukti Digital (LPBD)”** sebagai persyaratan untuk mencapai gelar Magister Komputer pada Program Magister Informatika, Pasca Sarjana Fakultas Teknologi Industri Universitas Islam Indonesia.

Pada kesempatan ini dengan penuh kerendahan hati penulis haturkan ucapan terima kasih yang tak terhingga dan penghargaan yang setinggi-tingginya kepada kedua orang tua saya serta dan alm kakek dan nenek, beserta keluarga besar Panende, Adjimalaha yang senantiasa memotivasi dan tiada henti memberi doa dan kasih sayangnya kepada penulis.

Di samping itu, secara khusus penulis haturkan terima kasih kepada:

1. Rektor UII Yogyakarta, Bapak Nandang Sutrisno, S.H.,M.Hum.,LLM.,Ph.D dan para Pembantu Rektor.
2. Bapak Dekan Fakultas Teknologi Industri, Dr.R. Teduh Dirgahayu,ST.,M.Sc dan Ibu Wakil Dekan Dr. Sri Kusumadewi, S.Si.,MT, atas motivasi, koreksi dan kemudahan pelayanan selama studi.
3. Bapak Dr. R. Teduh Dirgahayu, ST.,M.Sc. sebagai Ketua Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia.
4. Bapak Dr. Imam Riadi, M.Kom. Selaku dosen pembimbing 1, Terima kasih atas segala bantuan dukungan, semangat dan pengetahuannya serta kemudahan yang diberikan selama pembuatan tesis ini.
5. Bapak Yudi Prayudi, S.Si.,M.Kom. Selaku dosen pembimbing 2 sekaligus sebagai orang tua penulis selama masa kuliah, Terima kasih atas segala bantuan, dukungan, semangat dan pengetahuannya serta kemudahan yang diberikan selama masa perkuliahan hingga akhir studi.
6. Bapak Dr. Bambang Sugiantoro, M.T. Selaku dosen penguji yang telah memberikan motivasi dan semangat serta bimbingan yang sangat berarti bagi penulis dalam menyelesaikan tesis ini.
7. Krisna Widatama, S.Kom.,CHFI.,CEH selaku teman diskusi, teman kosan yang senantiasa menjadi teman yang baik sekaligus saudara.

8. Seluruh Dosen dan civitas Magister Teknik Informatika, baik secara langsung maupun tidak langsung telah membantu penulis selama masa studi penulis.
9. Staf Administrasi dan tata usaha Magister Teknik Informatika, Universitas Islam Indonesia, yang telah membantu dalam segala urusan administrasi di kampus.
10. Yulita Setiawati Belike, S.Ked yang selalu memberikan semangat serta motivasi di beberapa bulan terakhir ini.
11. Rekan-rekan mahasiswa MTI khususnya FD angkatan XIV yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lain.
12. Semua pihak yang telah membantu penulis selama penyusunan tesis ini yang tidak dapat penulis sebutkan satu persatu.

Semoga Allah SWT senantiasa memberikan berkat dan anugrah-Nya berlimpah bagi beliau-beliau yang tersebut di atas. Sangat disadari dalam tesis ini terdapat banyak kekurangan oleh karena itu semua saran dan kritik penulis terima dengan lapang dada demi kesempurnaan penulisan tesis ini. Akhirnya harapan penulis semoga tesis ini bermanfaat bagi kita semua.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, April 2018

Mohamad Fadli Panende, S.Kom

Daftar Isi

Lembar Pengesahan Pembimbing.....	i
Lembar Pengesahan Penguji	ii
Abstak	iii
Pernyaraan Keaslian Tulisan.....	iv
Daftar Publikasi	v
Halaman Kontribusi	vi
Halaman Persembahan.....	vii
Kata Pengantar.....	viii
Daftar Isi.....	xi
Daftar Tabel.....	xiii
Daftar Gambar	xiv
Glosarium.....	xvii
BAB 1 Pendahuluan.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
BAB 2 Landasan Teori	5
2.1 Tinjauan Pustaka.....	5
2.2 Bukti Digital	13
2.3 Konsep Akses Kontrol LPBD.....	14
2.4 <i>Attribute Based Access Control (ABAC)</i>	15
2.5 XACML.....	16
BAB 3 Metodologi Penelitian	18
3.1 Studi Pustaka.....	18
3.2 Gambaran Umum ABAC	19
3.2.1 Rancangan Model Data <i>Flow</i> ABAC LPBD	20
3.2.2 Konsep XACML <i>Policy</i> Elemen <i>Subject</i>	21

3.2.3 Konsep XACML <i>Policy</i> Elemen <i>Resource</i>	22
3.2.4 Konsep XACML <i>Policy</i> Elemen <i>Actions</i>	23
3.2.5 Konsep XACML <i>Policy</i> Elemen <i>Environment</i>	24
3.2.6 Rancangan Alur ABAC LPBD	26
3.3 Implementasi.....	28
3.4 Simulasi dan Skenario.....	28
3.5 Pengujian	28
3.6 Hasil dan Analisa	29
3.6 Kesimpulan	29
 BAB 4 Pembahasan	 31
4.1 <i>Policy Statement</i>	31
4.2 XACML Policy LPBD	34
4.3 Output XACML Policy	49
4.3.1 <i>Output XACML Policy Subject</i>	50
4.3.2 <i>Output XACML Policy Resource</i>	52
4.3.3 <i>Output XACML Policy Actions</i>	54
4.3.4 <i>Output XACML Policy Environment</i>	56
4.4 <i>Source Code</i> Pembacaan	59
4.5 Implementasi.....	61
4.5.1 Implementasi ABAC Pada Sistem LPBD.....	62
4.5.2 Spesifikasi Komputer yang Digunakan	64
4.5.3 Jenis <i>Complier</i>	65
4.6 Simulasi dan Skenario.....	66
4.7 Pengujian Akses Kontrol.....	67
4.7.1 Pengujian Kondisi Permit	67
4.7.2 Pengujian Kondisi Deny	70
4.8 Hasil dan Analisis	72
4.8.1 Hasil.....	72
4.8.2 Analisis	73
 BAB 5 Penutup.....	 79
5.1 Kesimpulan	79
5.2 Saran.....	79
 Daftar Pustaka	 80

Daftar Tabel

Tabel 2.1.....	7
Tabel 4.1.....	31
Tabel 4.2.....	57
Tabel 4.3.....	62
Tabel 4.4.....	63
Tabel 4.5.....	65
Tabel 4.6.....	65
Tabel 4.7.....	71
Tabel 4.8.....	72
Tabel 4.9.....	74
Tabel 4.10.....	75
Tabel 4.11.....	76

Daftar Gambar

Gambar 2.1	13
Gambar 2.2	16
Gambar 3.1	18
Gambar 3.2	19
Gambar 3.3	20
Gambar 3.4	21
Gambar 3.5	22
Gambar 3.6	23
Gambar 3.7	24
Gambar 3.8	26
Gambar 3.9	27
Gambar 3.10	27
Gambar 3.11	29
Gambar 3.12	29
Gambar 4.1	33
Gambar 4.2	33
Gambar 4.3	34
Gambar 4.4	34
Gambar 4.5	35
Gambar 4.6	36
Gambar 4.7	37
Gambar 4.8	38
Gambar 4.9	39
Gambar 4.10	40
Gambar 4.11	40
Gambar 4.12	41
Gambar 4.13	42
Gambar 4.14	42
Gambar 4.15	43
Gambar 4.16	44
Gambar 4.17	45
Gambar 4.18	46

Gambar 4.19	47
Gambar 4.20	47
Gambar 4.21	48
Gambar 4.22	49
Gambar 4.23	49
Gambar 4.24	50
Gambar 4.25	51
Gambar 4.26	51
Gambar 4.27	52
Gambar 4.28	53
Gambar 4.29	53
Gambar 4.30	54
Gambar 4.31	54
Gambar 4.32	55
Gambar 4.33	55
Gambar 4.34	56
Gambar 4.35	56
Gambar 4.36	57
Gambar 4.37	57
Gambar 4.38	58
Gambar 4.39	59
Gambar 4.40	62
Gambar 4.41	62
Gambar 4.42	65
Gambar 4.43	65
Gambar 4.44	67
Gambar 4.45	68
Gambar 4.46	69
Gambar 4.47	69
Gambar 4.48	70
Gambar 4.49	71
Gambar 4.50	71
Gambar 4.50	72
Gambar 4.50	74

Glosarium

CoC	- Chain of Custody
XACML	- eXtensible Access Control Markup Language
ABAC	- Attribute Based Access Control
RABAC	- Rule Attribute Based Access Control
RBAC	- Rule Based Access Control
ACL	- Access Control List
DAC	- Directory Access Control
MAC	- Mandatory Access Control
AR-ABAC	- Attribute Rule – Attribute Based Access Control
LPDB	- Lemari Penyimpanan Bukti Digital
QoS	- Quality of Service
SOA	- Service Oriented Architecture
OSN	- Online Social Networks
SAML	- Security Assertion Markup Language
ACPO	- Association of Chief Police Officer
DEC	- Digital Evidence Cabinet

BAB 1

Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini sangat pesat, hal ini berbanding lurus dengan tingkat kejahatan yang terjadi *cybercrime*. Dengan demikian dapat dipastikan bahwa perkembangan teknologi informasi ini tidak hanya memberikan dampak positif bagi pengguna, melainkan juga dampak negatif. Berdasarkan data dari Polda Metro Jaya terdapat 1.207 kasus *cybercrime* pada tahun 2016 dengan 699 kasus yang telah terselesaikan. Data ini menunjukkan bahwa *cybercrime* sudah menjadi permasalahan yang sangat serius di era digital ini.

Salah satu faktor penting dalam sebuah proses investigasi sebuah kasus *cybercrime* yaitu hal yang terkait dengan barang bukti (Prayudi, 2014), dalam hal ini yang dimaksud yaitu barang bukti elektronik dan barang bukti digital. Bukti elektronik adalah barang bukti yang bersifat fisik dan dapat dikenali secara visual seperti (komputer, handphone, camera, CD, harddisk, dll) sedangkan bukti digital adalah barang bukti yang berisi informasi-informasi digital hasil ekstraksi dari bukti elektronik. Bukti digital terbagi menjadi dua kategori (Marshall, 2008), yaitu *closed system* dan *open system*. Bukti digital merupakan alat bukti yang sah dipengadilan, seperti yang dijelaskan oleh (Prayudi & Priyambodo, 2015) dalam penelitiannya bahwa informasi-informasi digital yang tersimpan didalam perangkat elektronik dapat digunakan sebagai alat bukti yang sah sebagaimana diatur dalam UU ITE Nomor 11 Tahun 2008 Pasal 5 Ayat 1 yang berbunyi “Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Untuk itu bukti digital yang ditemukan dalam sebuah kasus kejahatan harus tetap terjaga keasliannya, agar dapat dipertanggung jawabkan dipengadilan .

Sejumlah penelitian yang telah dilakukan sebagai upaya untuk mengimplementasikan konsep penanganan bukti digital. Namun demikian mengingat karakteristik barang bukti digital terus berkembang dan semakin kompleks maka munculah salah satu solusi yang ditawarkan (Prayudi & Ashari, 2014) yaitu model *digital evidence cabinets* sebagai pendekatan baru yang diimplementasikan dalam penanganan bukti digital dan *chain of custody*. Solusi ini diorientasikan untuk memberikan penyelesaian masalah penyimpanan bukti digital. Model tersebut telah diimplentasikan (Widatama, 2017) dalam bentuk sistem Lemari Penyimpanan Bukti Digital (LPBD). Namun sayangnya sistem

tersebut masih dalam tahap awal dan belum dilengkapi dengan rancangan akses kontrol yang baik.

Lemari penyimpanan bukti digital seharusnya dibuat tidak hanya berdasar pada permasalahan-permasalahan tentang manajemen bukti digital saja, akan tetapi komponen-komponen penting lainnya dalam lemari penyimpanan bukti digital itu sendiri yaitu pengaturan pada aksesnya, sehingga skema atau desain akses kontrol *policy* terhadap Lemari Penyimpanan Bukti Digital ini menjadi sangat penting.

Beberapa kemungkinan solusi model akses kontrol yang sudah pernah ada sebelumnya seperti *discretionary access control* (DAC), *mandatory access control* (MAC), *access control list* (ACL), serta *rule based access control* (RBAC) dll, untuk mengatasi permasalahan akses kontrol pada lemari penyimpanan bukti digital ini digunakan model *attribute based access control* (ABAC) sebagai generasi baru dari generasi sebelumnya karena konsep tersebut memiliki fleksibilitas terhadap desain akses kontrol dan juga merupakan pengembangan dari akses kontrol yang pernah ada sebelumnya. Akses kontrol terhadap lemari penyimpanan bukti digital tidak cukup hanya ditangani oleh mekanisme autentikasi dan authorisasi *user* saja. Autentikasi, authorisasi dan akses kontrol memiliki fungsi dan tujuan yang berbeda walaupun pada implementasinya terlihat seolah-olah sebuah proses tunggal. Menurut (Younis, Kifayat, & Merabti, 2013) autentikasi fokusnya pada verifikasi terhadap klaim identitas *user*, authorisasi fokusnya pada pemberian hak akses terhadap *resource*, sementara akses kontrol fokusnya pada proteksi keamanan dari *resource* tertentu, yaitu sebuah mekanisme untuk memastikan bahwa *user* tidak melakukan tindakan tertentu yang tidak sesuai dengan *policy* umum keamanan yang diterapkan. Akses kontrol melindungi sistem dan sumber daya dari akses yang tidak berhak dan menentukan tingkat authorisasi setelah prosedur autentikasi berhasil dilengkapi (Stallings & Brown, 2015).

Akses kontrol yang ada pada LPBD saat ini hanya berupa proses autentifikasi dan authorisasi pada *username* dan *password* saja, sementara model akses kontrol yang ditawarkan merupakan proses autentifikasi dan authorisasi yang lebih kompleks yaitu dengan menerapkan *policy* sebagai pengaturan aksesnya.

Mengingat belum adanya skema rancangan model akses kontrol yang baik pada lemari penyimpanan bukti digital ini, maka perlu dilakukan perancangan model akses kontrol *policy* menggunakan pendekatan *attribute based access control* yang akan mendukung kebutuhan lemari penyimpanan bukti digital itu sendiri. Hasil akhir dari penelitian ini adalah terciptanya model *attribute based access control* berupa akses kontrol

policy untuk memberikan hak akses bagi pengguna yang diberi kewenangan menangani bukti digital yang ada pada lemari penyimpanan bukti digital.

1.2 Rumusan Masalah

Berdasarkan permasalahan pada latar belakang, maka dapat diambil beberapa rumusan masalah yaitu:

1. Bagaimana membangun sebuah rancangan *attribute based access control* (ABAC) pada lemari penyimpanan bukti digital (LPBD).
2. Bagaimana menguji kinerja rancangan akses kontrol yang dibangun untuk meningkatkan tingkat keamanan sistem LPBD pada proses autentifikasi dan autentikasi *user*.

1.3 Batasan Masalah

Batasan-batasan masalah pada penelitian ini adalah:

1. Penelitian ini hanya dilakukan terkait pada pengembangan sebuah rancangan akses kontrol pada lemari penyimpanan bukti digital menggunakan pendekatan *attribute based access control* (ABAC) dan XACML sebagai bahasa pemrogramannya.
2. Akses hanya diberikan kepada beberapa aktor yaitu *first responder, investigator, officer, dan lawyer*

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Membangun rancangan akses kontrol pada Lemari Penyimpanan Bukti Digital.
2. Melakukan pengujian terhadap keamanan Lemari Penyimpanan Bukti Digital dalam segi pemberian hak akses pada pengguna.

1.5 Manfaat Penelitian

Manfaat yang dihasilkan dari penelitian ini adalah sebagai berikut:

1. Memberikan kemudahan bagi para pejabat pengelola bukti digital dalam melakukan investigasi khususnya dalam menjaga autentifikasi bukti digital yang ada.
2. Membantu pihak-pihak terkait untuk mendokumentasikan bukti digital sehingga dapat dipertanggungjawabkan secara hukum di pengadilan.
3. Sebagai referensi bagi peneliti lain yang mengambil kajian penelitian yang sama dan sebagai wawasan untuk mengembangkan penelitian selanjutnya.

BAB 2

Landasan Teori

2.1 Tinjauan Pustaka

Terdapat beberapa penelitian yang telah dilakukan berkaitan dengan ABAC. Penelitian pertama yang dilakukan oleh (Dan & Yuan, 2012) yang mengangkat permasalahan sistem kontrol akses lintas domain ABAC, bersama dengan domain keamanan sebagai atribut dengan subjek, objek, otoritas, atribut lingkungan sebagai dasar untuk akses pengambilan keputusan.

Penelitian kedua dilakukan oleh (Burmester, 2013) mengangkat isu tentang model akses kontrol berbasis atribut *real-time* yang memperluas fungsionalitas ABAC dengan menggunakan atribut *real-time* yang mencerminkan persyaratan aplikasi kritis, mereka mengatakan dua model aplikasi mereka (a) sistem gardu induk, dan (b) sistem *cyber*-fisik medis). Penelitian ketiga dilakukan oleh (Qi et al., 2016) Membahas tentang model *rule attribute based access control* (RABAC) dalam, penelitian ini menganalisis secara mendalam kekurangan-kekurangan pada model RABAC yang ada, dan mengusulkan model RABAC yang lebih baik dibanding dengan model yang ada. Model yang diusulkan telah ditingkatkan sampai tingkat tertentu dalam granularitas dan fleksibilitas akses kontrol.

Penelitian keempat dilakukan oleh (Son Ha, Luong Khiem, & Dang, 2016) penelitian ini berfokus pada permintaan penulisan ulang yang menerima tanggapan yang tidak sesuai dengan mengurangi sumber daya yang diperlukan untuk diselaraskan dengan kebijakan sistem. Mereka membuat model baru memanfaatkan Framework XACML 3.0 untuk mengetahui kebijakan yang paling sesuai untuk setiap permintaan masukan dalam empat aspek, termasuk tindakan, subjek, lingkungan dan sumber daya untuk permintaan menulis ulang. Penelitian selanjutnya dilakukan oleh (Riad, Yan, Hu, & Ahn, 2015) dalam penelitian ini menyajikan sebuah model akses kontrol berbasis *attribute rule* yang di implementasikan pada *cloud computing*, dalam penelitian ini dikatakan bahwa model yang mereka usulkan mendukung *attribute rules* yang berkaitan dengan hubungan antara pengguna dan objek, serta kemampuan mengakses objek berdasarkan tingkat sensitivitasnya. Penelitian selanjutnya yaitu (Nasim & Buchegger, 2014) yang mengangkat *issue* tentang model akses kontrol menggunakan XACML dalam penelitian ini dikatakan bahwa mereka bertujuan untuk memberika dasar bagi sistem perlestarian privasi yang dibangun dari komponen ringan dan mudah tersedia yaitu XACML dan SAML (*Security Assertion Markup Language*) dengan otentikasi rahasia, termasuk cara sederhana untuk merumuskan kebijakan akses

untuk pengguna. Sebagai landasan pendukung, berikut merupakan penelitian yang dilakukan oleh (Prayudi & Ashari, 2014) yang mengangkat isu tentang pembuatan *digital evidence cabinet* untuk penanganan bukti digital. Penelitian tersebut dilanjutkan oleh (Widatama, 2017) yang mengimplemantasikan konsep DEC kedalam sebuah sistem penanganan bukti digital yang diberi nama LPBD atau lemari penyimpanan bukti digital. Selajutnya adalah rangkuman dan perbandingan terhadap penelitian yang dilakukan sebelumnya dapat dilihat pada tabel 2.1.

Tabel 2.1 Perbandingan Penelitian Terdahulu

No.	Paper	Isu	Solusi	Metode	Solusi
1	2	3	4	5	6
1.	(Burmester, 2013)	Model Akses kontrol berbasis atribut waktu (T-ABAC)	Pembuatan akses kontrol berbasis waktu <i>real-time</i> (T-ABAC)	<ol style="list-style-type: none"> 1. Peninjauan kembali model akses kontrol yaitu <i>Traditional Access Control Model</i> terutama berfokus pada kerahasiaan dan integritas 2. Quality of Service (QoS) Arsitektur memperluas layanan <i>Best Effort</i> untuk pengguna akhir jaringan IF dalam hal keterlambatan Quality of Service (QoS) 	Menyajikan model ABAC, dimana attribute <i>real-time</i> dapat mempertimbangkan prioritas akses
2.	(Dan & Yuan, 2012)	Model akses kontrol lintas domain	Pembuatan akses kontrol lintas domain berbasis ABAC	<ol style="list-style-type: none"> 1. Pendekatan <i>Service Oriented Architecture</i> (SOA), yang memiliki fleksibilitas untuk mengatur dan mengelola distribusi sumber daya dalam manajemen domain yang berbeda 2. Pendekatan <i>Attribute Based Access Control</i> (ABAC) karena di anggap yang lebih halus dalam pengendalian akses. 	Menyajikan sistem akses kontrol lintas domain berbasis ABAC, bersama dengan domain keamanan sebagai atribut dengan subjek, objek, otoritas atribut lingkungan sebagai dasar akses pengambilan keputusan,

Tabel 2.1 Perbandingan Penelitian Terdahulu (Lanjutan)

1	2	3	4	5	6
					menghilangkan hambatan integrasi untuk kerangka kerja SOA
3.	(Son Ha et al., 2016)	Model akses kontrol berbasis solusi	Pembuatan akses kontrol berbasis solusi Rew-XAC	<p>Pendekatan yang digunakan dalam penelitian ini adalah:</p> <ol style="list-style-type: none"> 1. Rew-XAC yaitu model akses kontrol yang dapat menerapkan proses penulisan ulang. 2. Framework XACML 3.0 adalah <i>eXtensible Access Control Markup Language</i> untuk membangun model baru Rew-XAC. 	<p>Model akses kontrol berbasis solusi dilingkungan perubahan kebijakan, yaitu <i>modification on each request</i> dengan <i>Not Applicable</i> yang artinya merespon berdasarkan kebijakan sistem. Lebih tepatnya model tersebut mencegah respon “not applicable” dan menghitung nilai kebijakan <i>fuzzy</i> berdasarkan kebutuhan pemilik permintaan.</p>

Tabel 2.1 Perbandingan Penelitian Terdahulu (Lanjutan)

1	2	3	4	5	6
4.	(Riad et al., 2015)	Model akses kontrol berbasis atribut untuk Cloud Computing	Membangun sebuah model akses kontrol berbasis atribut baru yang mendukung atribut aturan untuk Cloud Computing	<ol style="list-style-type: none"> 1. <i>Attribute-Rule</i> atau (AR-ABAC) untuk menentukan kesepakatan tentang jenis atribut apa yang harus digunakan dan berapa banyak atribut yang harus diperimbangkan dan memperhitungkan keputusan akses 2. Pemberian peran spesifik berdasarkan atribut yang dimiliki untuk dapat mengakses objek. 3. Pemanfaatan <i>Cloud Computing's Infrastructures-as-a-Services</i> (IaaS) dan menyediakan empat cara yang berbeda untuk pengaksesannya 	Menyajikan usulan model akses kontrol AR-ABAC

Tabel 2.1 Perbandingan Penelitian Terdahulu (Lanjutan)

1	2	3	4	5	6
5.	(Qi et al., 2016)	Model akses kontrol berdasarkan peran dan atribut	Merancang model akses kontrol berbasis peran dan atribut serta implementasinya	RABAC untuk memfasilitasi pengolahan peraturan akses kontrol oleh administrator	Akses kontrol dapat mengoptimalkan pilihan dalam memisahkan kode kebijakan, dengan demikian mempermudah pengolahan kebijakan.
6.	(Nasim & Buchegger, 2014)	Model Akses kontrol berbasis XACML	Merancang model akses kontrol berbasis XACML untuk desentralisasi <i>Online Social Networks</i> (OSN)	Menggunakan kombinasi bahasa <i>eXtensible Access Control Markup Language</i> (XACML) dan <i>Security Assertion Markup Language</i> (SAML) dengan otentikasi rahasia untuk menyembunyikan struktur data	Memberikan aturan dinamis untuk akses kontrol yang disesuaikan dengan OSN yang dapat diterapkan pada rincian yang berbeda dari masing-masing kiriman keseluruhan profil.
7.	(Prayudi, Ashari, & Priyambodo, 2014)	Penanganan pada bukti digital.	Pembuatan model Digital Evidence Cabinet.	Pembuatan Digital Evidence Cabinet menggunakan 3 pendekatan, yaitu: <i>digital evidence management frameworks</i> , <i>digital evidence bags</i> dan <i>secure communication</i> .	Tersimpannya bukti digital pada digital evidence cabinet dan pembatasan akses terhadap bukti digital

Tabel 2.1 Perbandingan Penelitian Terdahulu (Lanjutan)

1	2	3	4	5	6
8.	(Widatama, 2017)	Pengembangan konsep lemari penyimpanan bukti digital untuk mendukung implementasi digital <i>chain of custody</i> form.	Penyimpanan bukti digital yang dimodelkan seperti lemari penyimpanan pada bukti fisik. Serta pembatasan akses bukti digital berdasarkan peran petugas dalam penanganan kasus.	Penyimpanan bukti digital dimana informasi metadata bukti digital dan <i>chain of custody</i> disimpan pada struktur XML.	Lemari penyimpanan bukti digital yang dapat menghasilkan form digital <i>chain of custody</i> .
9.	Usulan konsep penelitian	Pengembangan konsep <i>attribute based access control</i> menggunakan struktur XACML	Memberikan hak akses pada setiap pihak yang diberi otorisasi menangani bukti digital dalam bentuk <i>access control policy</i> guna meningkatkan tingkat keamanan lemari penyimpanan bukti digital	<i>Access control policy</i> dimana dapat memferivikasi setiap <i>user</i> yang melakukan akses pada aplikasi lemari penyimpanan bukti digital berupa pemberian hak akses berbasis atribut <i>policy</i>	Sebuah model <i>access control policy</i> yang dapat memberikan hak akses kepada setiap pengguna yang berhak menangani bukti digital yang ada pada lemari penyimpanan bukti digital
		Sampai dengan saat ini belum adanya rancangan sebuah model akses kontrol yang secara khusus diperuntukan untuk sebuah lemari penyimpanan bukti digital berdasarkan atribut <i>policy</i> . Model akses kontrol yang ada pada lemari penyimpanan bukti digital saat ini hanya berupa proses otentifikasi sederhana yang pada umumnya digunakan pada sebuah sistem, hal ini akan berakibat pada bukti yang ada dapat dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab. Solusi dengan pendekatan akses			

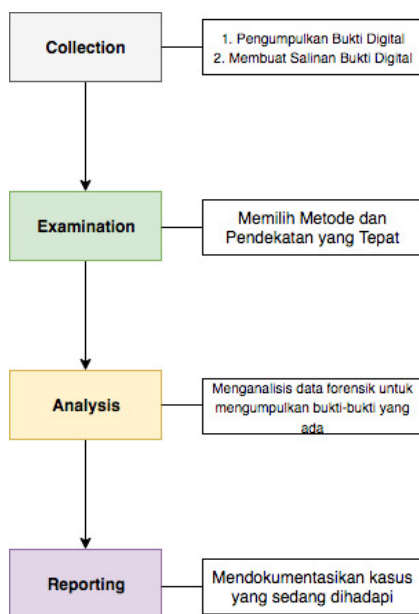
Tabel 2.1 Perbandingan Penelitian Terdahulu (Lanjutan)

1	2	3	4	5	6
		kontrol berbasis atribut <i>policy</i> ini diterapkan karena karakteristik pengguna sistem dan interaksinya tidak sederhana akses untuk pengguna biasa. Apabila pengguna biasa, maka akses terhadap sistem cukup difasilitasi dengan model autentifikasi sederhana. Namun model bisnis pada penegak hukum, khususnya untuk aktifitas investigasi digital sangat kompleks sehingga membutuhkan pengaturan dalam bentuk <i>access control policy</i> .			

2.2 Bukti Digital

Forensik digital dan bukti digital memiliki keterkaitan, namun keduanya memiliki definisi yang berbeda. Forensik digital adalah metode yang dapat dijelaskan secara ilmiah dan dapat dibuktikan. Tujuan dari aktivitas forensika digital ini adalah untuk menjaga, mengumpulkan memvalidasi, mengidentifikasi menganalisis, menafsirkan, mendokumentasikan dan menyajikan bukti digital yang terdokumentasi dalam bentuk *chain of custody* untuk dipresentasikan di pengadilan (Morioka & Sharbaf, 2016). Dalam prosedur forensik digital, terdapat prosedur dasar yang sering digunakan, yaitu: pengumpulan barang bukti *collection*, perawatan barang bukti *preservation*, *verification*, *analysis*, *interpretation*, *documentation* dan presentasi hasil di pengadilan *presentation*.

Pendapat lain tentang prosedur forensika digital, bahwa secara umum terdapat 4 proses utama dalam forensika digital, yaitu: *collection*, *examination*, *analysis* dan *reporting* (Dogan & Akbal, 2017). Gambar 2.1 adalah proses dari forensika digital:



Gambar 2.1 Proses Utama Forensika Digital

Berikut adalah penjelasan proses utama dalam forensika digital pada gambar 2.1.

1. *Collection*, bukti digital dikumpulkan dan dilakukan proses *imaging*.
2. *Examination*, mencari dan menentukan metode yang bertujuan untuk menguji bukti digital.

3. *Analysis*, langkah untuk menganalisis yang bertujuan untuk menemukan bukti digital yang sesuai dengan informasi yang dibutuhkan oleh otoritas yudisial atau keadilan.
4. *Reporting*, fase persiapan dokumentasi untuk diajukan ke otoritas pengadilan.

Sedangkan definisi bukti digital menurut (Harbawi & Varol, 2017) adalah jejak yang diinginkan maupun tidak diinginkan yang berasal dari perubahan data digital pada perangkat elektronik. Berdasarkan sumbernya, bukti digital terbagi menjadi 2 kategori (Marshall, 2008), yaitu *closed system* dan *open system*. *Closed system* merupakan sistem yang pernah terkoneksi internet. Artinya, sistem tersebut sangat terisolasi dan hanya terhubung dengan sistem pada komputer yang lain. Berbeda dengan *closed system*, *open system* merupakan sistem yang terhubung dengan internet meskipun sistem tersebut tidak terhubung dengan sistem pada komputer lain, contohnya ketika seseorang menghubungkan laptop pada WiFi.

Menurut ACPO (*Association of Chief Police Officer*) terdapat 4 prinsip dalam penanganan bukti digital. Berikut adalah 4 prinsip penanganan bukti digital menurut ACPO.

1. Prinsip 1, seorang penegak hukum tidak diperbolehkan untuk mengubah data yang terdapat pada komputer atau media penyimpanan karena hal ini akan dipertanggung jawabkan di pengadilan.
2. Prinsip 2, dalam situasi tertentu dan jika memang diharuskan, seseorang diperbolehkan untuk mengakses data yang asli, namun orang tersebut harus kompeten dan ia harus dapat menjelaskan tentang relevansi terhadap barang bukti serta implikasi terhadap kegiatan yang dilakukan terhadap barang bukti tersebut.
3. Prinsip 3, catatan dan audit yang berisi semua proses dalam penanganan barang bukti elektronik harus dibuat dan ketika pihak ketiga memeriksa catatan dan audit tersebut, hasilnya harus sama dengan yang dimiliki oleh pihak investigator.
4. Prinsip 4, orang yang bertanggung jawab dalam investigasi ini harus memastikan bahwa hukum dan semua prinsip ini dipatuhi oleh orang-orang yang terlibat.

2.3 Konsep Akses Kontrol Lemari Penyimpanan Bukti Digital

Munculnya konsep akses kontrol lemari penyimpanan bukti digital didasarkan atas permasalahan dalam pengaturan akses yang ada pada lemari penyimpanan bukti digital yang berkebutuhan dalam beberapa hal yaitu: model bisnis dari bagian-bagian yang berhubungan langsung dengan bukti digital, penyimpanan informasi metadata bukti digital maupun akses kontrol dan keamanan terhadap digital CoC (Widatama, 2017). Konsep ini diperkenalkan

oleh (Prayudi et al., 2014) dalam penelitiannya yang berjudul *Digital Evidence Cabinets : A Proposed Frameworks for Handling Digital Chain of Custody*. Dalam penelitiannya disebutkan bahwa lemari penyimpanan bukti digital merupakan sistem yang dibuat untuk penanganan CoC dari setiap bukti digital yang telah diperoleh. Konsep ini dibangun atas 3 pendekatan, yaitu: *Digital Evidence Management Frameworks*, kantong bukti digital dan keamanan.

2.4 Attribute Based Access Control (ABAC)

ABAC adalah sebuah metode akses kontrol dimana subjek hanya akan dapat melakukan *request* untuk menjalankan sebuah operasi terhadap objek didasarkan pada atribut yang disematkan pada subjek, objek, kondisi lingkungan serta kumpulan *policy* yang termasuk dalam atribut dan kondisinya. Pada sistem ABAC, elemen authorisasi didefinisikan dalam terminology atribut. Atribut itu sendiri adalah karakteristik dari entitas yang didefinisikan sebelumnya oleh pihak yang memiliki wewenang untuk itu. Menurut (Priebe et al. 2007), ide dasar utama dari ABAC adalah tidak memberikan *permission* sebagai *ouput* dari hubungan langsung antara subjek dan objek namun mendasari pemberian *permission* tersebut melalui atribut dari keduanya.

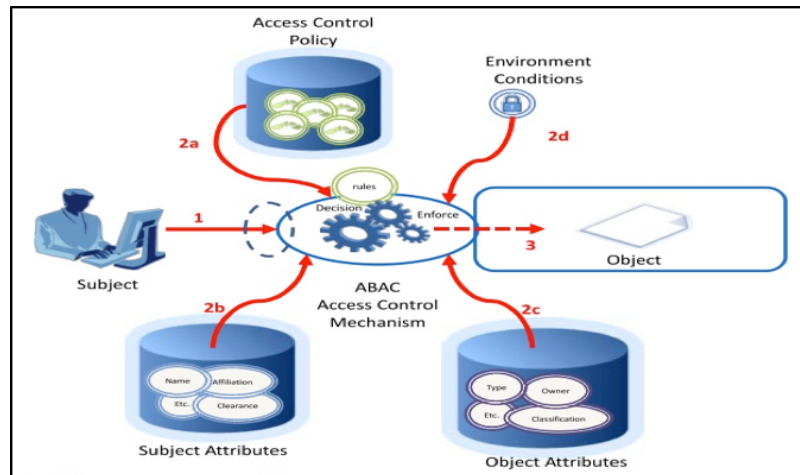
Salah satu fleksibilitas terhadap penggunaan ABAC sebagai model akses kontrol adalah adanya standar bahasa XML untuk mendukung desain akses kontrol *policy* dan penggunaan ABAC sebagai model akses kontrol, yaitu *extended access control XML language* yang disingkat dengan XACML. Menurut (Abd El-Aziz dan Kannan 2013), XACML adalah merupakan *policy language* yang memiliki kemampuan untuk mengkontruksi ekspresi dari serangkaian akses kontrol *policy* sehingga dapat menjelaskan : “*who can do what and when*”.

Selanjutnya menurut (Sandhu, 2010), terdapat 4 aspek atribut dalam ABAC, yaitu :

- *Subject* adalah pengguna manusia ataupun non manusia misalnya (*device* ataupun komponen *software*) yang meminta *request access*. Contoh dari atribut untuk *subject* adalah : nama, tanggal lahir, alamat rumah, pekerjaan. Sementara itu *request access* dapat menggunakan *attribute* individual dari *subject* atau kombinasinya untuk menunjukkan identitas yang unik.
- *Resource* adalah sesuatu target yang dilindungi seperti halnya *device, files, record, table*, proses, program, jaringan.

- *Actions* adalah eksekusi dari suatu fungsi pada saat melakukan *request* dari sebuah *subject* terhadap *resource*. Sebagai contoh, *actions* terhadap *file* data akan melibatkan *creation*, *modification* dan *deletion*.
- *Environment attribute* adalah karakteristik dari operational ataupun situational seperti misalnya *current time*, *current temperature*, *IP address*.

Adapun gambaran umum cara kerja ABAC dapat terlihat pada gambar 2.2.



Gambar 2.2 Gambaran Umum Cara Kerja ABAC

Gambar 2.2 menjelaskan (hu et al. 2014) cara kerja dari ABAC dapat dijelaskan sebagaimana ilustrasi pada gambar 2.2 berdasarkan ilustrasi tersebut maka terdapat 3 langkah utama untuk menerapkan ABAC, yaitu:

- Subject* meminta *request* kepada *object*
- Pemberian *decision* diberikan melalui mekanisme evaluasi terhadap *rules*, *subject attribute*, *object attribute* dan *kondisi environment*.
- Subject* diberikan *decision: deny* atau *permit* untuk akses terhadap *object*

2.5 XACML

XACML (*eXtensible Access Control Markup Language*) adalah standar dari OASIS untuk menspesifikasikan ABAC *policy* menggunakan format XML. Terdapat 4 atribut *predefined* yaitu : *subject*, *resource*, *action* dan *environment*. Namun *type* atribut *user* dapat juga diterapkan untuk aplikasi tertentu. XACML mendukung berbagai *type data*, *type nama* serta *path expression* untuk atribut misalnya : *string*, *integer*, *internet-based names*, *regular*

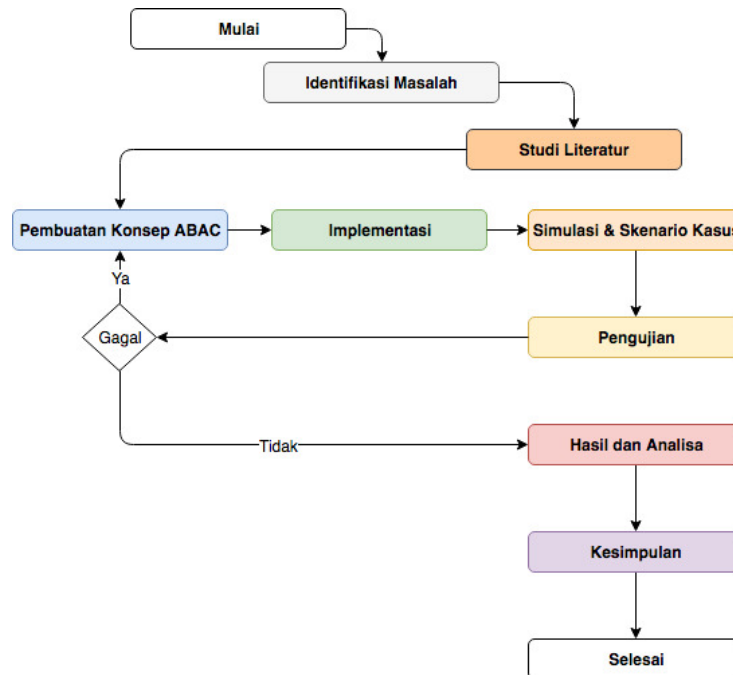
expression dan XPATH. Dalam hal penggunaan atribut, *type* data lebih utama dispesifikasikan dibandingkan dengan domain (Abd El-Aziz & Kannan, 2013).

XACML menyediakan mekanisme modularisasi untuk mengatasi *policy* yang kompleks. Pada satu sisi, spesifikasi XACML adalah bersifat *hierarchical*, memuat satu atau lebih himpunan *policy* dan setiap himpunan *policy* memiliki daftar *rules*. Penggunaan *multiple policy* dimungkinkan untuk mendukung *collaborative policy administration*, misalnya pada beberapa departmen yang berbeda dan dapat pula dibagi dalam sub *policy* yang lebih kecil untuk mengurai kompleksitas *policy*. Sementara pada sisi yang lain komponen target yang direpresentasikan oleh *attribute matching condition* menyediakan *level* abstraksi dan meningkatkan *performance* dari *attribute matching*.

BAB 3

Metodologi Penelitian

Bab ini menjelaskan tentang alur penelitian dengan menjabarkan setiap proses yang dibuat secara sistematis. Hal ini agar permasalahan yang dihadapi dapat terselesaikan, hasil dan kesulitan-kesulitan yang ditemukan saat proses penelitian sedang berlangsung dapat dianalisis. Alur penelitian dapat dilihat pada gambar 3.1.



Gambar 3.1 Alur Penelitian

Gambar 3.1 menjelaskan bahwa metodologi penelitian tersebut digunakan berdasarkan *review* dari penelitian yang terkait sebelumnya. Metodologi penelitian tersebut bertujuan untuk mengembangkan penelitian yang sudah pernah ada sebelumnya. Dalam penelitian ini dilakukan analisis untuk mengetahui tahapan-tahapan apa saja yang diterapkan dalam pembuatan model ABAC pada LPBD dan diuji coba agar dapat menghasilkan kesimpulan pengembangan dan pemanfaatan yang baik. Metodologi penelitian ini meliputi 8 tahapan utama yaitu *identifying research problem*, studi literature, pembuatan konsep ABAC, implementasi, simulasi dan skenario kasus, pengujian, hasil dan analisa, serta membuat sebuah kesimpulan berkaitan dengan hasil perancangan ABAC pada LPBD ini.

3.1 Studi Pustaka

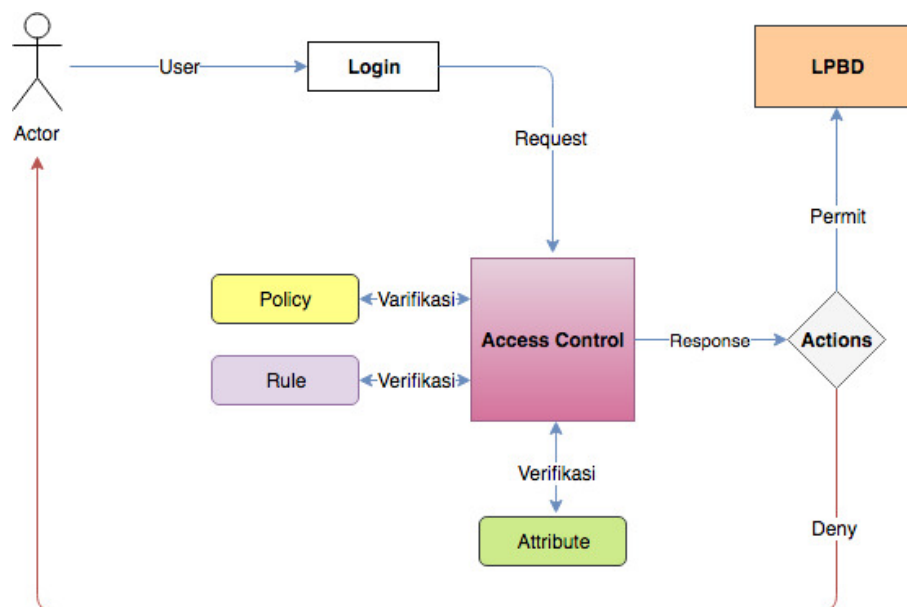
Studi pustaka dilakukan pada langkah awal untuk menghimpun informasi yang relevan dengan topik atau masalah yang akan diteliti. Sumber-sumber informasi pada studi pustaka

dapat diperoleh melalui buku-buku yang memiliki keterkaitan dengan masalah yang akan diteliti, jurnal ilmiah serta sumber-sumber informasi lainnya yang dapat diperoleh melalui internet. Informasi-informasi yang di dapat juga dapat diperoleh dengan menghadiri seminar-seminar ilmiah yang sering diadakan oleh beberapa universitas.

Penelitian ini membutuhkan studi pustaka untuk mendapatkan semua informasi tentang konsep *attribute based access control* yang dianalogikan sebagai alat akses kontrol pada penyimpanan bukti digital. Sedangkan pada bahasa pemrograman XACML, studi pustaka yang dibutuhkan adalah teori-teori XACML yang berkaitan dengan aturan penulisan pada bahasa XACML.

3.2 Gambaran Umum *Attribut Based Access Control* (ABAC) LPBD

Tahapan setelah terkumpulnya informasi melalui tahapan studi pustaka adalah tahapan pembuatan konsep *attribute based access control* pada LPBD. Perancangan konsep ini dimulai dengan gambaran umum cara kerja sistem akses kontrol yang dimana akan dibangun, pada tahapan ini terlihat adanya pembagian hak akses yang diberikan pada setiap pihak yang berwenang untuk mengakses sistem lemeri penyimpanan bukti digital tersebut terlihat pada gambar 3.2.



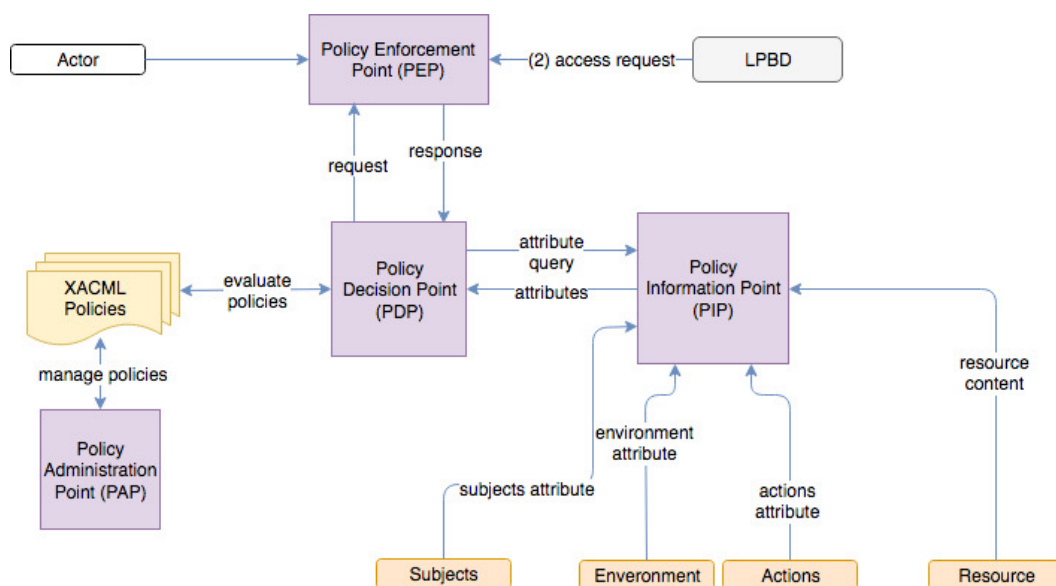
Gambar 3.2 Gambaran umum perancangan ABAC LPBD

Gambaran umum perancangan *attribute based access control* (ABAC) pada lemari penyimpanan bukti digital (LPBD) dianalogikan sebagai sebuah proses *login* yang dimana

proses autentifikasinya melalui *rule policy* yang disematkan pada aktor sebagai subjek dan aplikasi sebagai objek, rancangan gambaran umum ABAC LPBD ini merupakan pengembangan dari konsep akses kontrol yang sudah ada sebelumnya, konsep perancangan akses kontrol ini harus dapat mengidentifikasi setiap pengguna yang mengakses aplikasi . Identifikasi tersebut didasarkan atas *rule policy* yang akan dibuat setelah perancangan selesai digambarkan. *Rule policy* tersebut tersimpan dalam bentuk struktur XACML. Setelah rancangan gambaran umum ABAC LPBD digambarkan maka tahapan selanjutnya adalah menjelaskan tentang desain atribut *policy* sebagai landasan pengaturan akses untuk setiap pengguna. Berikut adalah konsep desain *policy* dan pengaturan akses pengguna yang diberikan izin untuk melakukan *login* pada lemari penyimpanan bukti digital.

3.2.1 Perancangan Model Data Flow XACML Policy LPBD

Setelah perancangan gambaran umum ABAC LPBD dibuat maka langkah selanjutnya yaitu pembuatan model data flow XACML *policy* sistem LPBD. *Policy language* digunakan untuk menjelaskan kebutuhan pengontrolan akses secara umum dan memiliki *standard extension points* (SEP) untuk mendefinisikan fungsi baru, *type* data, kombinasi logika, dan lain-lain. *Request* atau *response language* digunakan untuk membentuk sebuah *query* untuk mengevaluasi apakah suatu tindakan diizinkan atau tidak untuk dilakukannya akses ataukah untuk menginterpretasikan hasil Sebagaimana yang terlihat pada gambar 3.2.



Gambar 3.3 Model Data Flow XACML Policy LPBD

XACML LPBD *data flow model* merupakan gambaran logika yang terlibat dalam melakukan pemrosesan terhadap sebuah permintaan akses. Seperti yang terlihat pada Gambar 3.2 *policy enforcement point* (PEP) sebagai pelaksana awal ketika dilakukannya permintaan akses, selanjutnya akan memberikan *request* terhadap *policy decision point* (PDP) yang bertugas berperan sebagai yang memutuskan permintaan, selanjutnya *policy information point* (PIP) yang berperan sebagai yang menampung 4 jenis atribut yaitu *subject*, *resource*, *actions*, dan *environment*. *Policy decision point* (PDP) dalam hal ini bertugas untuk mengevaluasi XACML *policies* yang berada pada *policy administration point* (PAP) yang disini juga bertugas sebagai yang mengelola XACML *policy* tersebut.

3.2.2 Konsep XACML Policy Elemen Subject

Konsep XACML *Policy* pada elemen subjek ini merupakan pengembangan dari kebutuhan kontrol yang ada pada sistem LPBD, atribut *subject* dirancang bertujuan agar setiap *user* dapat melakukan permintaan akses sesuai dengan atribut yang akan disematkan pada elemen tersebut. Sebagaimana yang terlihat pada gambar 3.3.

```

<PolicyId>= → Diisi dengan nama policy
  <Target>
    <Ruleeffect>= → Diisi dengan nama rule dan effect yang akan digunakan
      <Target>
        (Subjects) → Berisi nilai atribut policy subjek
          <SubjectMatch → Berisi nilai subject match
            <AttributeValue → Berisi nilai data type yang akan digunakan
              <SubjectAttributeDesignator → Berisi nilai attributeId dan type data
            </SubjectMatch
          </Subject
        </Target
      </Rule>
    </Policy>

```

Gambar 3.4 Konsep XACML *Policy Attribute* Elemen *Subject*

Gambar 3.4 menjelaskan tentang bagaimana konsep XACML elemen *subject* sistem LPBD yang dimana *PolicyId* sebagai *root* elemen yang diberi nama *policy example* elemen ini mempunyai sub elemen yaitu *rule* sub elemen berisi nilai *effect* yang akan digunakan dan *ruleId* merupakan nama *rule* yang akan dibuat, selanjutnya elemen ini mempunyai sub

elemen yang bernama *target* sub elemen target berfungsi untuk menentukan nilai atribut mana yang akan dieksekusi ketika *request* dilakukan, sub elemen ini juga memiliki sub elemen yang bernama *subject* yang berfungsi menampung nilai atribut *subject*. Elemen *subject* mempunyai atribut yang bernama *subject match*, atribut ini berisi nilai atribut *matchId* yang akan digunakan. *Subject match* memiliki sub atribut yang bernama *attribute value* yang berisi nilai *type* data yang akan digunakan dan *subject attribute designator* yang berisi atribut yang akan disematkan pada elemen *subject* itu sendiri.

3.2.3 Konsep XACML Policy Elemen Resource

Setelah konsep XACML *policy* atribut elemen *subject* dijelaskan maka akan dilanjutkan dengan merancang atribut yang berisi komponen - komponen elemen *resource* sebagaimana yang terlihat pada gambar 3.5 yaitu konsep XACML *policy* atribut elemen *resource*.

```

<PolicyId> → Diisi dengan nama policy
  <Target>
    < Rule combining algorithm → Berisi kombinasi algoritma yang digunakan
    <Rule effect → Diisi dengan nama rule dan effect yang akan digunakan
    <Target>
      (Subjects) → Berisi nilai atribut policy subjek
      <SubjectMacth → Berisi nilai subject macth
      <AttributeValue → Berisi nilai data type yang akan digunakan
      <SubjectAttributeDesignator → Berisi nilai attributeId dan type data
    </SubjectMatch
  </Subjects
  (Resources) = → Berisi atribut policy resource
    <ResourceMatch → Berisi nilai resource match
      <Attribute Value → Berisi nilai type data yang akan digunakan
      <ResourceAttributeDesignator → Berisi attributeId & type data
    </ResourceMatch
  </Resources>
</Target
<Rule>
</Policy>

```

Gambar 3.5 Konsep XACML Policy Attribute Elemen Resource

Gambar 3.5 menjelaskan tentang konsep XACML *policy* atribut elemen *resource* yang merupakan kelanjutan dari konsep XACML *policy* atribut elemen *subject*. Tahapan ini dimana elemen *resource* mempunyai sub elemen yang bernama *resource match* atau *matchId* yang berisi nilai atribut yang nantinya akan digunakan serta memiliki atribut yang bernama *attribute value* yang akan diisi dengan *type data* dan nilai atribut berupa *string* selain itu atribut selanjutnya yaitu *resource attribute designator* atribut ini berfungsi sebagai *attributeId* atribut ini berisi nilai *resource* yang akan digunakan dan mempunyai *type data* sebagai *schema* pada *resource*.

3.2.4 Konsep XACML Policy Elemen Actions

Langkah selanjutnya adalah menjelaskan konsep XACML *policy* atribut elemen *actions*. Atribut ini berfungsi meneruskan perintah *request* yang sudah dijelaskan pada bagian sebelumnya, berikut konsep XACML *policy* atribut elemen *actions* yang terlihat pada gambar 3.6.

```

<PolicyId> → Diisi dengan nama policy
<Target>
  < Rule combining algorithm → Berisi kombinasi algoritma yang digunakan
  <Rule effect → Diisi dengan nama rule dan effect yang akan digunakan
  <Target>
    (Subjects) → Berisi nilai atribut policy subjek
      <SubjectMacth → Berisi nilai subject macth
      <AttributeValue → Berisi nilai data type yang akan digunakan
      <SubjectAttributeDesignator → Berisi nilai attributeId dan type data
    </SubjectMatch
  </Subjects
  (Resources) → Berisi atribut policy resource
    <ResourceMatch → Berisi nilai resource match
      <AttributeValue → Berisi nilai type data yang akan digunakan
      <ResourceAttributeDesignator → Berisi attributeId & type data
    </ResourceMatch
  </Resources>
  (Actions) → Berisi nilai atribut policy actions
    <ActionMatch → Berisi nilai actions match
      <AttributeValue → Berisi nilai type data yang akan digunakan
  
```

```

    <ActionsAttributeDesignator → Berisi attributeId & type data
  </ActionMatch>
</Actions>
</Target>
<Rule>
</Policy>

```

Gambar 3.6 konsep XACML *Policy Attribute Actions*

Gambar 3.6 menjelaskan bahwa atribut *action* berisi nilai atribut elemen *actions* yang bernama *action match* atau *matchId* yang nilai fungsinya akan diisi dengan nilai *string-equal* atribut ini berfungsi melakukan operasi yang akan dilakukan pada *resource* seperti membaca, menulis, menghapus dll. Atribut yang akan menjadi *action access* pada *subject* berada pada sub atribut yang bernama *attribute value* atribut yang disimpan berupa *type data* yang akan diisi dengan nilai dari *type data* itu sendiri.

3.2.5 Konsep XACML *Policy Elemen Environment*

Sebagai konsep XACML *policy* bagian terakhir yang akan melengkapi struktur-struktur sebelumnya elemen *environment* juga menjadi bagian yang penting dalam merancang sebuah pengaturan akses menggunakan XACML *policy*, sebagaimana yang terlihat pada gambar 3.7.

```

<PolicyId> → Diisi dengan nama policy
  <Target>
    < Rule combining algorithm → Berisi kombinasi algoritma yang digunakan
    <Rule effect → Diisi dengan nama rule dan effect yang akan digunakan
    <Target>
      (Subjects) → Berisi nilai atribut policy subject
        <SubjectMacth → Berisi nilai subject macth
          <AttributeValue → Berisi nilai data type yang akan digunakan
          <SubjectAttributeDesignator → Berisi nilai attributeId dan type data
        </SubjectMatch
      </Subjects
      (Resources) → Berisi nilai atribut policy resource
        <ResourceMatch → Berisi nilai resource match
          <AttributeValue → Berisi nilai type data yang akan digunakan

```

```

        <ResourceAttributeDesignator → Berisi attributeId & type data
    </ResourceMatch>
</Resources>
(Actions) → Berisi nilai atribut policy actions
    <ActionMatch → Berisi nilai actions match
        <AttributeValue → Berisi nilai type data yang akan digunakan
    </ActionMatch>
</Actions>
(Environment) → Berisi nilai atribut policy environment
    <EnvironmentMatch → Berisi nilai environment match
        <AttributeValue → Berisi nilai type data yang akan digunakan
        <EnvironmentAttributeDesignstor → Berisi attributeId & type data
    </EnvironmentMatch>
</Environment>
</Target>
<Rule>
</Policy>

```

Gambar 3.7 konsep XACML *Policy Attribute* Elemen *Environment*

Konsep XACML *policy* elemen *environment* ini menjelaskan tentang fungsi dari elemen *environment* tersebut. Elemen ini berfungsi untuk mengumpulkan informasi mengenai konteks akses yang mungkin digunakan dalam membuat keputusan akses seperti *time*, *ip address*, *mac address* dll. Elemen *environment* mempunyai sub elemen yang bernama *environment match* yang akan diisi dengan nilai yang ada pada *environment match* itu sendiri, sub elemen ini mempunyai atribut yang bernama *attribute value* yang akan diisi dengan nilai *type data* yang akan digunakan yaitu *string*, selanjutnya elemen ini juga mempunyai *attribute value* yang berisi *type data* bernilai *string* dan *environment attribute designator* yang berisi nilai atribut *type data*, *attributeId*, dan *issuer*.

Berikut adalah daftar *user* yang nantinya akan diasumsikan sebagai aktor yang akan melakukan akses pada sistem lemari penyimpanan bukti digital.

1. First Responder

First responder memiliki kemampuan yang sama dengan investigator (Koch, 2008)

First responder berperan sebagai orang yang pertama mengunggah bukti digital.

2. Investigator

Investigator merupakan orang yang melakukan investigasi bukti digital terhadap kasus yang sedang dihadapi. Ia hanya diberikan akses untuk mengunduh bukti digital.

3. Officer

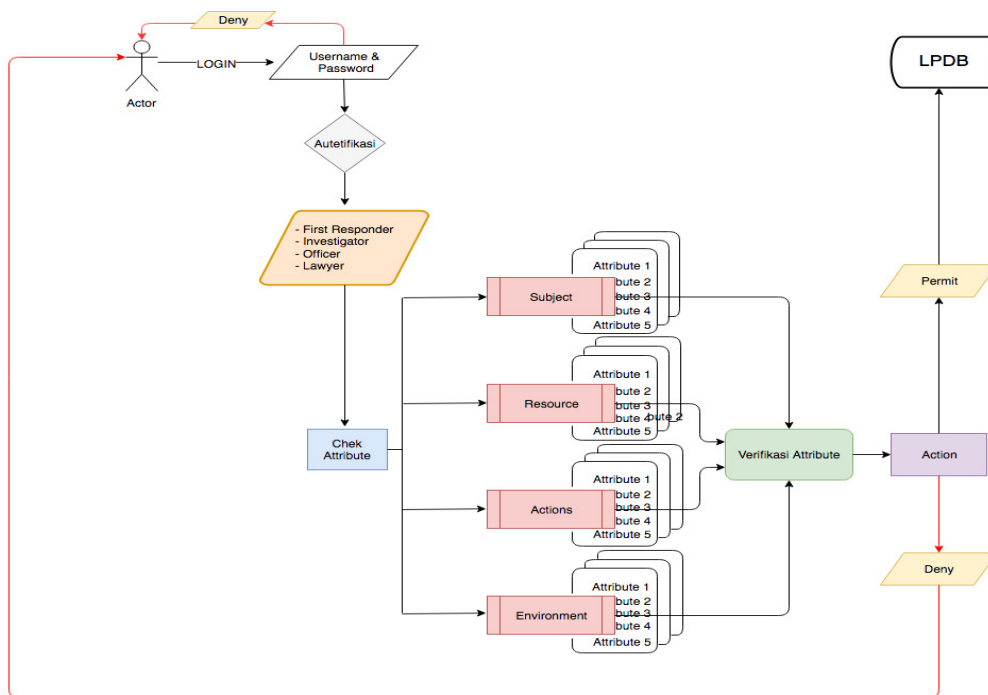
Officer memiliki peran sebagai pengatur hak akses terhadap LPBD. Selain itu, ia memiliki akses untuk mencetak form *chain of custody*.

4. Pengacara

Pengacara merupakan seorang yang melakukan atau memberikan nasihat dan pembelaan bagi orang lain yang berhubungan dengan penyelesaian suatu kasus hukum. Ia hanya diberi akses untuk mengunduh bukti digital hasil investigasi.

3.2.6 Rancangan Alur ABAC LPBD

Rancangan alur ABAC ini digambarkan bertujuan untuk menjelaskan secara detail, tentang bagaimana saat proses dilakukannya akses pada sistem lemari penyimpanan bukti digital dilakukan. Sebagaimana yang terlihat pada gambar 3.8 alur akses kontrol lemari penyimpanan bukti digital.



Gambar 3.8 Alur akses kontrol LPBD

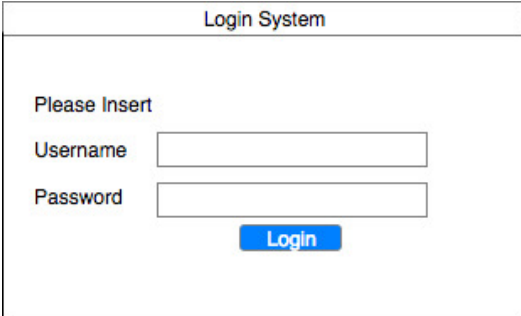
Gambar 3.8 menjelaskan tentang rancangan rancangan akses kontrol yang akan dibangun pada lemari penyimpanan bukti digital, yaitu bagaimana seorang aktor melakukan proses login pada LPBD, pada saat memasukkan *username* dan *password* sistem dengan otomatis

akan melakukan autentifikasi apakah benar *username* dan *password* yang dimasukan merupakan identitas dari salah satu aktor yang telah di daftarkan, selanjutnya jika *username* dan *password* yang dimasukan merupakan identitas dari salah satu aktor yang ada, maka sistem akan mencari tau siapa aktor yang memiliki *username* dan *password* tersebut, jika sudah diketahui siapa pemiliknya maka masuk pada proses pengecekan atribut pemilik identitas tersebut apakah sudah sesuai dengan kebijakan yang diberikan atau tidak, verifikasi atribut meliputi kecocokan atribut berdasarkan *subject*, *resource*, *operation*, dan *environment*. Jika identitas tersebut memenuhi persyaratan kebijakan yang telah diberikan maka *action* yang akan diterima yaitu *permit* atau pengguna diijinkan untuk masuk pada sistem lemari penyimpanan bukti digital. *Action deny* akan terjadi pada dua kemungkinan yaitu pertama jika *username* dan *password* yang di masukan tidak terdaftar dalam sistem, kedua jika saat proses verifikasi berjalan tidak dapat memenuhi persyaratan kebijakan salah satu atribut yang ada, maka proses *login* dinyatakan *deny* atau tidak bisa masuk pada sistem lemari penyimpanan bukti digital.

Pada struktur pembuatan rancangan ABAC ini adalah bagaimana ABAC menerapkan *rule policy* setiap pengguna yang masuk kedalam sistem. Seperti proses *login* pada sistem lemari penyimpanan bukti digital, yang akan melalui *rule policy* pada saat pengguna memasukan *username* dan *password*, secara otomatis sistem akan memverifikasi *rule policy* yang telah dimasukan sesuai dengan ketentuan yang ada.

3.2.7 Perancangan Desain Halaman Antar Muka

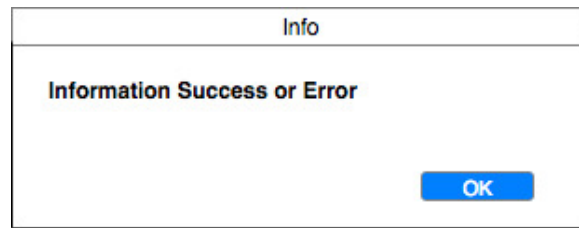
Perancangan desain halaman antarmuka ini dilakukan untuk membuat tampilan yang sederhana sehingga dapat dengan mudah digunakan. Perancangan desain antarmuka dilakukan dengan menggambar secara sederhana tampilan yang akan dibuat. Gambar 3.9 menunjukkan konsep desain halaman *login* sistem LPBD



The image shows a conceptual design for a login system interface. It is enclosed in a rectangular border with the title "Login System" at the top center. Below the title, the text "Please Insert" is displayed. Underneath, there are two input fields: the first is labeled "Username" and the second is labeled "Password". Below these fields is a blue button with the text "Login" in white.

Gambar 3.9 Konsep desain halaman *login*

Gambar 3.10 merupakan desain halaman informasi *login* untuk mengetahui berhasil atau gagal masuk kedalam sistem.



Gambar 3.10 Halaman Information

3.3 Implementasi

Tahapan ini merupakan aktivitas untuk pembuatan model *attribute based access control* pada lemari penyimpanan bukti digital berdasarkan perancangan yang telah dibuat sebelumnya. Hal ini untuk memastikan bahwa akses kontrol dapat dijalankan sebagaimana mestinya. Pada tahap ini, pembuatan rancangan akses kontrol lemari penyimpanan bukti digital menggunakan bahasa pemrograman Python, XACML 2.0 , UMU XACML Editor 132 dan Wing 101 sebagai *compiler*.

3.4 Simulasi dan Skenario Kasus

Tahapan simulasi kasus merupakan tahapan untuk membuat skenario tertentu yang bertujuan untuk membuat kesesuaian antara kebutuhan akses kontrol dengan sistem. Simulasi kasus ini berupa sebuah rancangan akses kontrol pada lemari penyimpanan bukti digital.

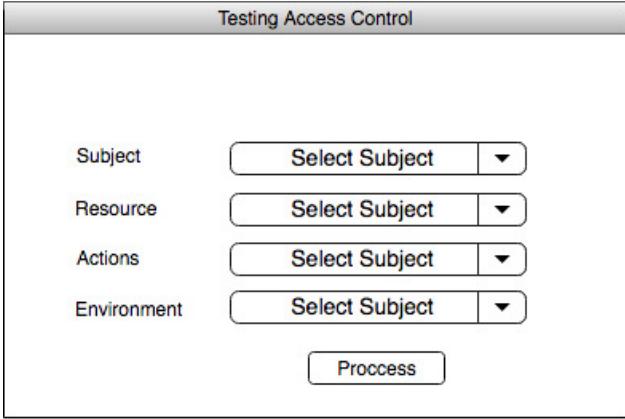
3.5 Pengujian

Tahapan pengujian merupakan tahapan yang penting untuk dilakukan saat melakukan tahapan perancangan dan implementasi. Pengujian dilakukan untuk memastikan akses kontrol dapat berjalan dengan baik sesuai dengan perancangan. Hasil dari perancangan tersebut selanjutnya akan dianalisis kelayakannya untuk digunakan pada lemari penyimpanan bukti digital.

Pengujian yang dilakukan adalah pengujian fungsionalitas. Adapun pengujian fungsionalitas meliputi kemampuan menerapkan *rule policy* untuk proses *login* pada sistem, mampu mengidentifikasi setiap pengguna yang melakukan akses pada aplikasi. Akses kontrol yang di bangun harus berjalan dengan baik ketika diuji. Selain itu, sistem juga harus mampu memilah pengguna yang masuk berdasarkan atribut yang ada ketika *username* dan

password yang dimasukkan. Hal ini bertujuan untuk meningkatkan keamanan sistem lemari penyimpanan bukti digital yang diakses oleh orang yang tidak memiliki kepentingan.

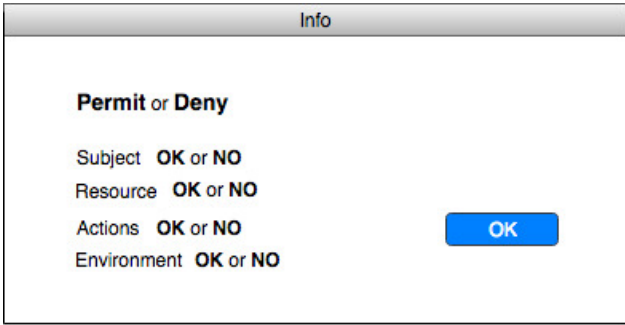
Rangkaian pengujian terhadap akses kontrol, dilakukan menggunakan sebuah *tools* pengujian. *tools* tersebut berisi aktivitas pengujian yang dilakukan terhadap sistem. Berikut adalah skema *tools* pengujian terhadap akses kontrol lemari penyimpanan bukti digital, sebagaimana yang terlihat pada gambar 3.10.



The image shows a window titled "Testing Access Control". It contains four rows of input fields, each with a "Select Subject" button and a dropdown arrow. The rows are labeled "Subject", "Resource", "Actions", and "Environment". Below these fields is a "Process" button.

Gambar 3.11 Konsep Halaman Aktivitas Pengujian Sistem

Selain halaman aktifitas pengujian terdapat juga halaman informasi hasil dari isian atribut. Sebagaimana yang terlihat pada gambar 3.11.



The image shows a window titled "Info". It displays the results of the test under the heading "Permit or Deny". The results are: Subject OK or NO, Resource OK or NO, Actions OK or NO, and Environment OK or NO. There is an "OK" button on the right side.

Gambar 3.12 Konsep Halaman Informasi Pengujian

3.6 Hasil dan Analisa

Tahap pada ini merupakan tahap ketika akses kontrol dianalisa dan dinyatakan lulus uji. Akses kontrol dinyatakan lulus uji dengan melihat sistem pengujian aktivitas. Setelah dinyatakan lulus uji, langkah berikutnya adalah penjelasan tentang kesimpulan dari keberhasilan akses kontrol yang telah dibuat.

3.7 Kesimpulan

Pada tahapan ini adalah tahapan pengambilan kesimpulan, setelah akses kontrol yang dibuat telah dianalisa dinyatakan lulus uji, langkah berikutnya adalah penjelasan tentang kesimpulan dari keberhasilan akses kontrol yang dibuat.

BAB 4

Pembahasan

4.1 Policy Statement LPBD

Policy statement yang dibangun berdasarkan ide dasar utama dari ABAC adalah tidak memberikan *permission* sebagai *ouput* dari hubungan langsung antara subjek dan objek namun mendasari pemberian *permission* tersebut melalui atribut dari keduanya (Priebe et al. 2007). Untuk itu perlu adanya sebuah usulan *policy statement* yang dimana akan menyesuaikan antara kebutuhan sistem dan kebutuhan akses kontrol. Dalam hal ini yang di maksud yaitu kebutuhan yang ada pada LPBD. Berikut adalah penjelasan *policy statement* LPBD:

1. First responder

First responder dapat melakukan aktivitas *login* pada LPBD ketika telah memenuhi komponen kebijakan yang diberikan, yaitu *subject* berisi identitas jabatan, dan *resource* berupa *upload digital evidence*, *create cabinet*, *create rack*, *create bag*, dan *input data case coc* serta *action* berupa *upload*, *create*, dan *input*. Pada *environment* berupa *ip address*, *time access*, dan *mac address*. Setelah dinyatakan dapat memenuhi semua kebijakan yang diberikan, maka dinyatakan dapat melakukan akses pada LPBD.

2. Investigator

Investigator dapat melakukan aktifitas *login* pada LPBD ketika dapat memenuhi komponen kebijakan yang diberikan seperti *subject* yang berisi identitas jabatan dan *resource* berupa *download digital evidence* dan *complete the data coc*. *Actions* berupa *download*, *complete data* dan *environment* berupa *ip address*, *time akses*, *mac address*. Setelah semua kebijakan yang ada terpenuhi maka dapat di ijinakan mengakses LPBD.

3. Officer

Officer dapat melakukan aktivitas *login* ketika dapat memenuhi persyaratan kebijakan yang diberikan berupa *subject* berisi atribut identitas jabatan, *resource* berupa *delete digital evidence*, *change password user*, *validate digital evidence*, *validate case status*, *download form coc*, *change code signature*, *validate data coc*. *Actions* berupa *delete*, *change password*, *validate*, *download*, *change code*. Dan *Environment* berupa *ip address*, *time access* dan *mac address*. Setelah semua kebijakan terpenuhi maka dapat diizinkan melakukan akses LPBD.

4. Lawyer

Lawyer Dapat melakukan aktivitas *login* pada LPBD ketika dapat memenuhi persyaratan kebijakan yang diberikan berupa *subject* berisi atribut identitas jabatan, *resource* berupa

download form coc, *action* berupa *download* dan *environment* berupa *ip address*, *time access*, dan *mac address*. Setelah semua kebijakan terpenuhi maka dapat diizinkan mengakses LPBD.

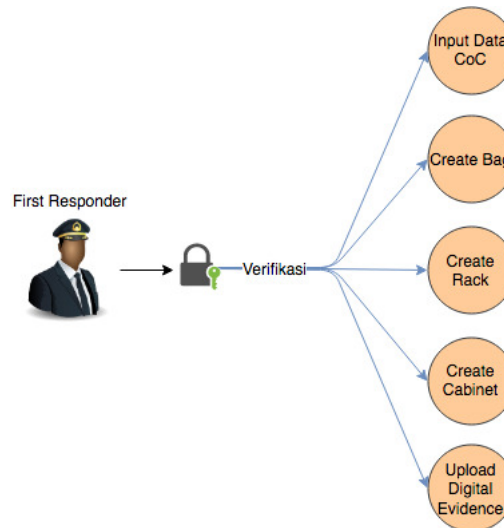
Policy dan *rule* mempunyai peran yang sangat penting dalam perancangan *attribute based access control* ini serta nilai apa saja yang akan disematkan pada setiap atribut yang ada pada elemen. Atribut berfungsi sebagai aturan *policy* pada saat *request* dilakukan. Berikut adalah usulan daftar atribut yang akan digunakan pada setiap elemen sebagaimana yang terlihat pada tabel 4.1.

Tabel 4.1 Daftar Usulan Atribut

Rule	Subject	Resource	Actions	Environment
Rules	First Responder	Upload Digital Evidence	Upload	1. Ip Address 2. Mac Address 3. Time Access
		Create Cabinet	Create	
		Create Rack	Create	
		Create Bag	Create	
		Input Data Case Coc	Input	
	Investigator	Download Digital Evidence	Download	1. IP Address 2. Mac Address 3. Time Access
		Complete The Data Coc	Complete Data	
	Officer	Delete Digital Evidence	Delete	1. IP Address 2. Mac Address 3. Time Access
		Change Password User	Change Password	
		Validate Digital Evidence	Validate	
		Validate Case Status	Validate	
		Download Form Coc	Download	
		Change Code Signature	Change Code	
		Validate Data Coc	Validate	
Lawyer	Download Form Coc	Download	1. IP Address 2. Mac address 3. Time Access	

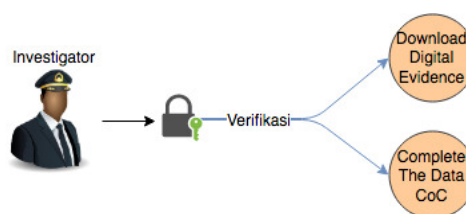
Tabel 4.1 menjelaskan bahwa dalam sebuah *policy* yang dibangun terdapat 1 *rule* yang diterapkan sebagai aturan akses pada LPBD, *rule* tersebut berisi ekspresi logika yang dirancang untuk memenuhi setiap *request*, komponen-komponen yang ada pada *rule* tersebut dianalogikan seperti contoh berikut. Ketika yang melakukan *request* adalah *user first responder* sebagai usur *subject* maka *resource* yang berhak di *access* yaitu *upload digital evidence*, *create cabinet*, *create rack*, *create bag* dan *input data coc* sebagai *attribute* dari *resource*, serta *action* yang diberikan berupa *download*, *create*, dan *input* sebagai atribut

dari *actions*. *Environment* berisi kondisi sumber daya saat *request* dilakukan yaitu *ip address*, *mac address* dan *time access* sebagai atribut dari *environment*. Gambar 4.1 merupakan detail gambar *policy statement*.



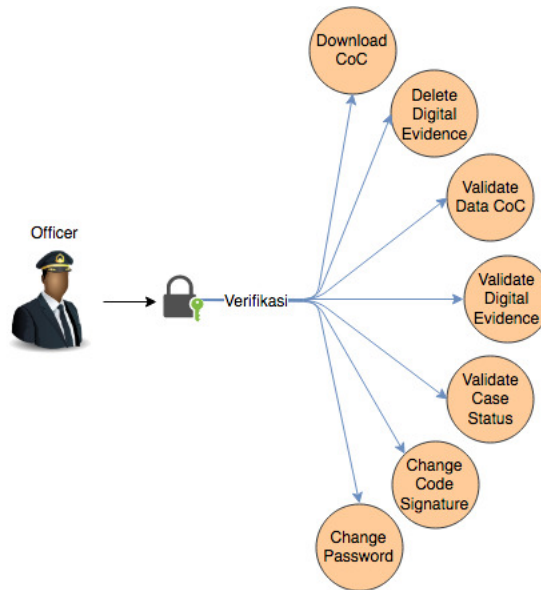
Gambar 4.1 *Policy Statement First Responder*

Gambar 4.1 Menjelaskan tentang detail *resource* yang berhak diakses oleh *user first responder* yang dalam hal ini diberikan wewenang untuk melakukan *input data coc*, *create bag*, *create rack*, *create cabinet*, dan *upload digital evidence*. Berbeda dengan *investigator* sebagai orang yang kedua setelah *first responder* dalam menangani barang bukti yang hanya diberikan dua hak akses *resource* sebagaimana yang terlihat pada gambar 4.2



Gambar 4.2 *Policy Statement Investigator*

Gambar 4.2 menjelaskan tentang detail *resource* yang diberikan kepada *user investigator* yaitu dua hak akses *resource* yang juga merupakan wewenang seorang investigator dalam menangani barang bukti digital berupa *download digital evidence*, dan *complete the data coc*. Selanjutnya sebagai yang paling banyak diberikan hak akses *resource* yaitu *user officer* yang diberikan tujuh hak akses *resource* sebagaimana yang terlihat pada gambar 4.3 berikut.



Gambar 4.3 *Policy Statement Officer*

Gambar 4.3 yaitu *policy statement officer* menjelaskan tentang detail hak akses *resource* yang diberikan pada *user officer* berupa *download coc*, *delete digital evidence*, *validate data coc*, *validate digital evidence*, *validate case status*, *change code signature*, dan *change password*. Selanjutnya yaitu penjelasan *policy statement user lawyer* sebagaimana yang terlihat pada gambar 4.4 berikut.



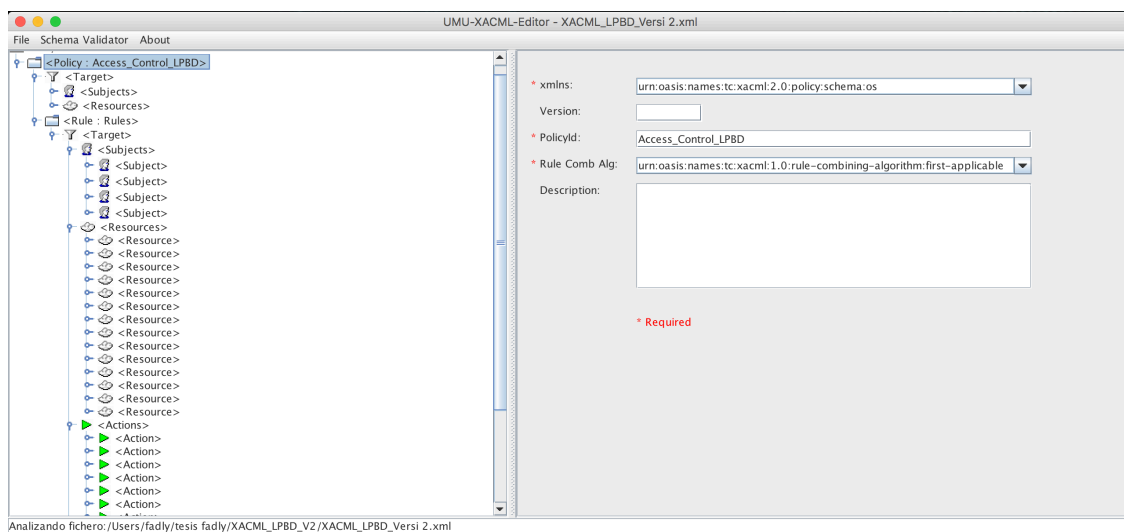
Gambar 4.4 *Policy Statement Lawyer*

Gambar 4.4 menjelaskan tentang *policy statement* pada *user lawyer* sebagai *user* yang paling sedikit diberikan hak akses *resource* yaitu hanya berupa *resource download coc*, hal ini disebabkan bahwa lawyer hanya merupakan seseorang yang dianggap sebagai tamu dan tidak mempunyai wewenang menangani barang bukti yang ada pada LPBD

4.2 XACML Policy LPBD

Struktur XACML *policy* dibangun berdasarkan kebutuhan-kebutuhan yang ada pada LPBD, struktur XACML *policy* ini dirancang menggunakan *tools* yang khusus untuk membuat sebuah XACML *policy*. *Tools* yang digunakan yaitu UMU-XACML-Editor Versi 1.3.2. penggunaan *tools* ini disebabkan UMU-XACML Editor dapat menjadi salah satu alternatif

untuk merancang sebuah struktur XACML yang akan dikeluarkan dalam bentuk *file* XML (Nergaard & Ulltveit-moe, 2015) yang nantinya akan digunakan sebagai *policy* ABAC pada LPBD ini. Proses pembuatan *policy* terbagi atas dua bagian yaitu menentukan *policy* target serta menentukan *rule* target hal ini bertujuan agar dapat dengan mudah menempatkan atribut yang akan disematkan pada setiap elemen yang ada seperti *subject*, *resource actions* dan *environment*. berikut adalah proses pembuatan struktur XACML *policy* LPBD yang diawali dengan perancangan target *policy* sebagaimana yang terlihat pada gambar 4.5 sebagai penjelasan awal untuk pembuatan struktur XACML *policy* LPBD.

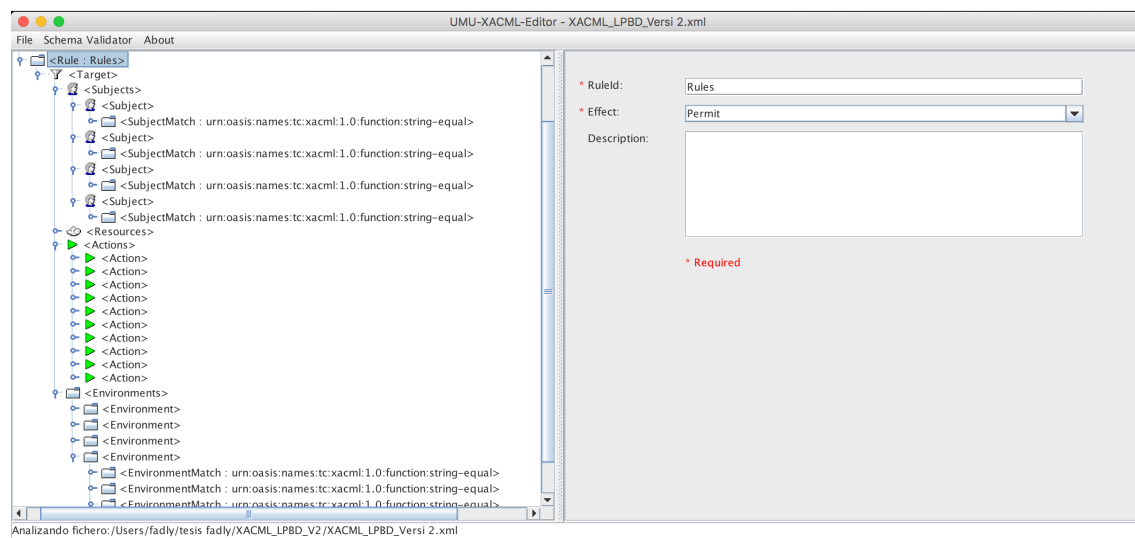


Gambar 4.5 XACML Policy Target

Gambar 4.5 menjelaskan bahwa letak fleksibilitas ABAC itu terdapat pada aturan *policy* dimana sebuah *resource* dapat dioperasikan lebih dari satu permintaan akses (Lorch, Proctor, Lepro, Kafura, & Shah, 2003). Penggunaan 1 *policy* dan 1 buah *rule* dikarenakan kebutuhan yang ada pada LPBD tidak mengharuskan untuk menggunakan lebih dari 1 *policy* dan *rule* yang menampung keseluruhan atribut yang disematkan pada *user*. Langkah pertama yang akan dilakukan yaitu menentukan nilai pada *policy target* yang juga merupakan *root* elemen pada rancangan *access control policy* LPBD ini, *policyId* diberi nama *access_control_policy_LPBD* dan *rule combining algorithm* diisi dengan nilai *first applicable* hal ini bertujuan karena *policy* LPBD mempunyai permintaan lebih dari 1 *rule*. Selanjutnya menjelaskan isi dari *target policy*, sebagaimana yang terlihat pada gambar diatas bahwa *target policy* ini berisi 4 *subject* yang artinya bahwa ke 4 *user* tersebut merupakan jumlah keseluruhan *user* yang diizinkan melakukan akses pada LPBD di antaranya yaitu , *first responder*, *investigator*, *officer*, dan *lawyer*. Selain *subject*, *target policy* juga berisi 15

resource yang artinya merupakan keseluruhan *resource* yang ada pada LPBD dan bisa di akses oleh *user* dengan ketentuan aturan yang ada pada *rule*.

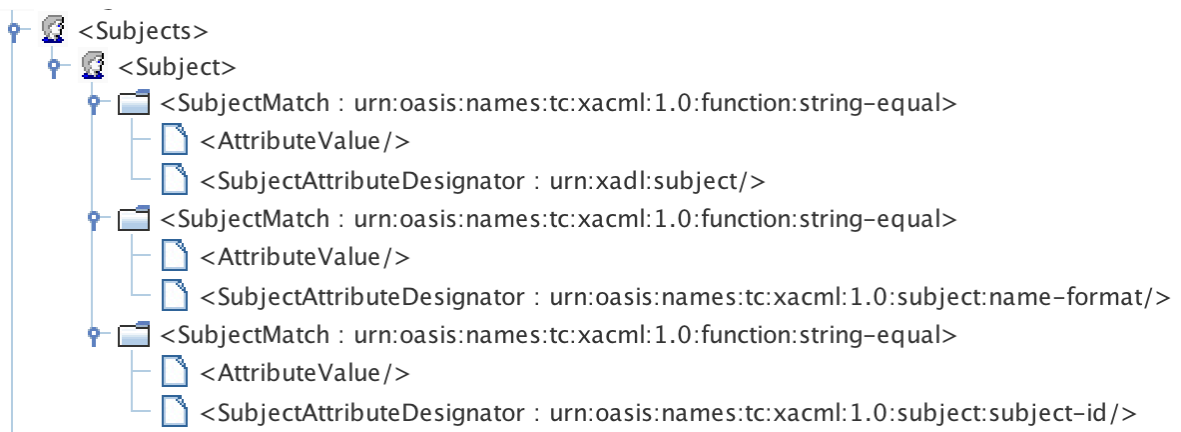
Selanjutnya yaitu menjelaskan tentang bagaimana rancangan *rule* yang menjadi sub elemen dari *root elemen policy* yang telah dijelaskan sebelumnya, sebagaimana yang terlihat pada gambar 4.6.



Gambar 4.6 Rancangan XACML Policy Rules

Gambar 4.6 menjelaskan bahwa *rule* dibuat berdasarkan aturan yang ada pada sistem LPBD yang bertujuan untuk mencegah terjadinya konflik antar elemen yang ada pada *policy* (Henim, 2016). Sebagai perancangan tahap ke 2 *policy* yang dibangun dimulai dengan menambahkan *rule* diberi nama *rules* yang dimana berisi aturan kebijakan yang diberikan kepada setiap *user* yang terdiri dari elemen *subject*, *resource*, *action*, dan *environment*. *Rules* tersebut diberi nilai *effect: permit* yang artinya *user* tersebut akan diizinkan mengakses sistem apabila dianggap memenuhi kebijakan yang diberikan, selanjutnya menentukan *target* yang menjadi kebijakan pada *user first responder* kebijakan yang diberikan terbagi menjadi 4 bagian atau 4 komponen elemen utama yang menjadi landasan perancangan *policy* ini. Yang pertama yaitu elemen *subject*, elemen ini berisi nilai atribut yang dimana nilai atribut tersebut mengandung informasi yang ada pada *user*, *subject match* yang ke-1 diisi dengan nilai *string-equal* dan mengisi nilai *attribute value* memiliki *data type:string*, selanjutnya mengisi *subject attribute designator* nilai *attributeId* diisi dengan nilai *subject* nilai *type data* diberi nilai *string* dan pada *issuer* diberi nama *first responder* yang menjadi jabatan dari *user*. Pada *subject match* yang ke-2 diberi nilai *function: string-equal* serta *attribute value* dan *type data* diberi nilai *string* serta *value* diberi nilai *assign*

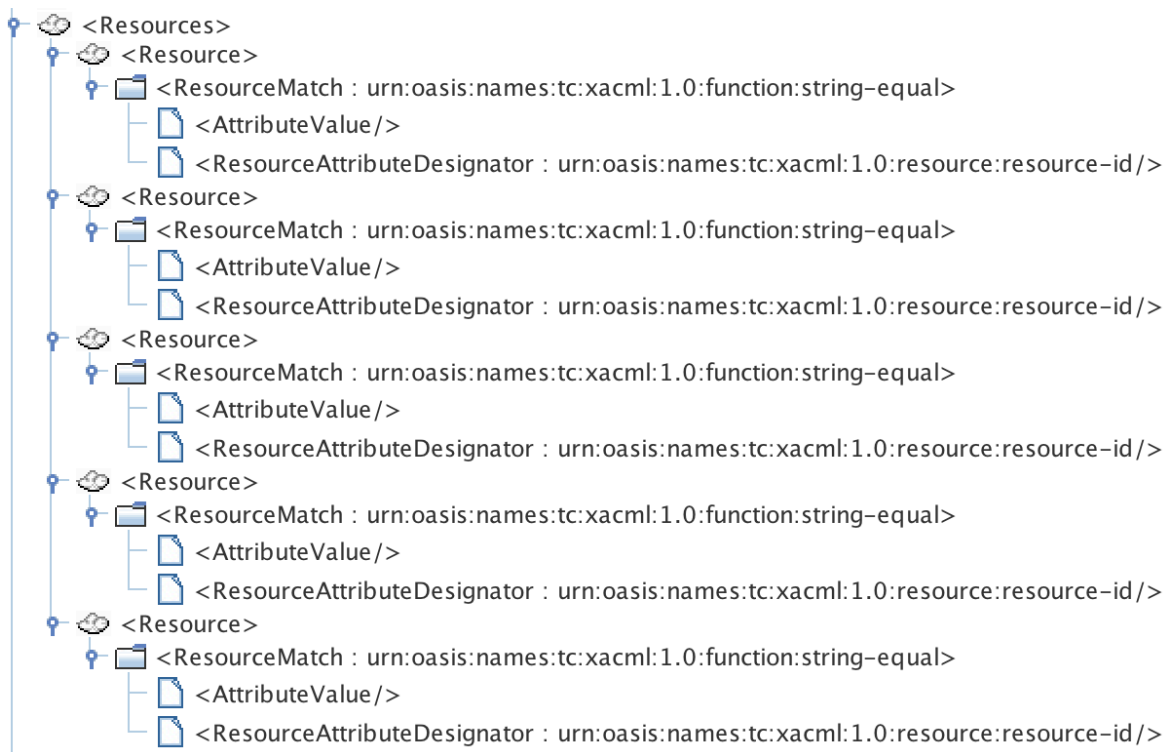
user, pada *subject attribute designator* diberi nilai *attributId: subject-name format* yang memiliki *type data: string* serta *issuer* diberi nama *fadly panende* yang akan menjadi *username* pada *user*. *Subject match* yang ke-3 diberi nilai *function: string-equal* serta *attribute value* memiliki *type data: string* dan *value* diberi nilai *assign user*, pada *subject attribute designator* diberi nilai *attributId: subject-id type data: string* serta *issuer* diberi nama *fadly123* yang akan menjadi *password* pada *user*. Gambar 4.7 merupakan detail isian elemen *subject first responder*.



Gambar 4.7 Detail Isian Elemen *Subject First Responder*

Tahapan selanjutnya yaitu menentukan atribut elemen *resource* yang bertujuan untuk menentukan *resource* apa saja yang berhak diakses (Hu et al., 2014) oleh *user first responder*. Diawali dengan menentukan nilai *resource match* yang ke-1 diberi nilai *function: string-equal* dan nilai *attribute value type data: string* dan *value* diberi nama *upload file digital evidence*. *Resource attribute designator* mempunyai *attributeId* yang diberi nilai *resourceId type data: string* serta *issuer* diberi nama *upload digital evidence*. Pada *resource match* yang ke-2 diberi nilai *function: string-equal* dan nilai *attribute value* memiliki *type data: string* dan *value* diberi nama *create new cabinet*. *Resource attribute designator* mempunyai *attributeId* diberi nilai *resourceId type data: string* serta *issuer* diberi nama *create cabinet*. *Resource match* yang ke- 3 diberi nilai *function: string-equal* dan nilai *attribute value* memiliki *type data: string* dan *value* diberi nama *create new rack* dan *resource attribute designator* mempunyai *attributeId* diberi nilai *resourceId type data: string* serta *issuer* diberi nama *create rack*. *Resource match* yang ke- 4 diberi nilai *function: string-equal* dan nilai *attribute value* memiliki *type data: string* dan *value* diberi nama *create new bag* dan *resource attribute designator* mempunyai *attributeId* diberi nilai *resourceId*

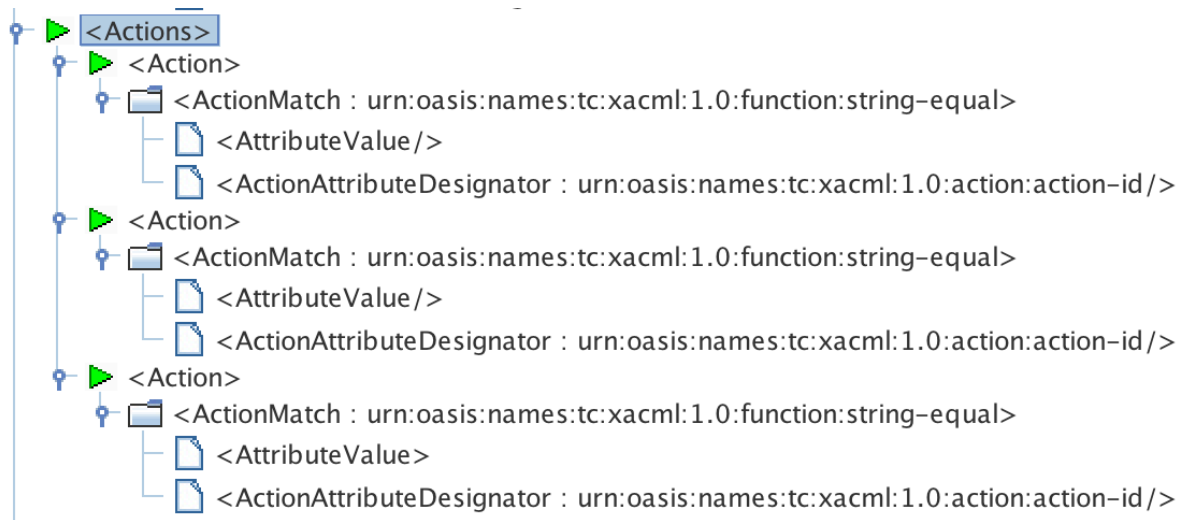
type data: string serta *issuer* diberi nama *create bag*. *Resource match* yang ke-5 diberi nilai *function: string-equal* dan nilai *attribute value* memiliki *type data: string* dan *value* diberi nama *input data case coc* dan *resource attribute designator* mempunyai *attributeId* diberi nilai *resourceId type data: string* serta *issuer* diberi nama *input data coc*. Gambar 4.8 adalah detail isian elemen *resource first responder*.



Gambar 4.8 Elemen *Resource First Responder*

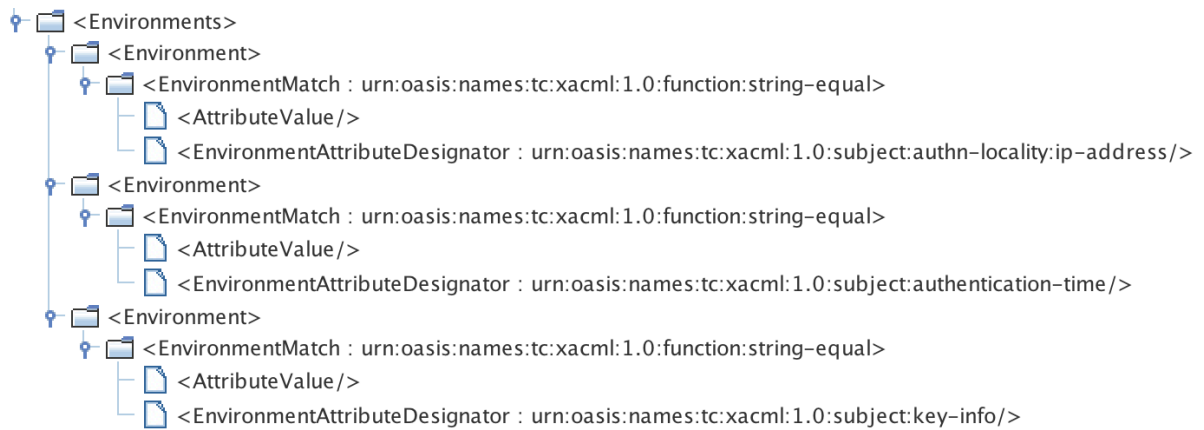
Langkah berikutnya yaitu merancang elemen *actions* yang bertujuan untuk menentukan *actions* yang diberikan (Hu et al., 2014) pada *user first responder*, elemen *actions* ini berfungsi menentukan operasi yang dilakukan pada *resource*. Diawali dengan menentukan nilai *action match* diberi nilai *function; string-equal* dan *form attribute value* memiliki *type data: string* dan *value* diberi nama *upload*. *Action attribute designator* memiliki *attributeId* diberi nilai *actionId type data: string* serta *issuer* diberi nama *upload file*. Elemen *actions* yang ke- 2, menentukan nilai *action match* diberinilai *function; string-equal* dan *form attribute value* memiliki *type data: string* dan *value* diberi nama *create* dan *action attribute designator* mempunyai *attributeId* diberi nilai *actionId type data: string* serta *issuer* diberi nama *create cabinet, rack, bag*. Elemen *actions* yang ke- 3. Diawali dengan menentukan nilai *action match* diberi nilai *function; string-equal* dan *attribute value* memiliki *type data: string* dan *value* diisi dengan *input* dan *action attribute designator*

mempunyai *attributeId* diberi nilai *actionId* type data: *string* serta *issuer* diberi nama *input data*. Gambar 4.9 merupakan detail isian elemen *actions first responder*.



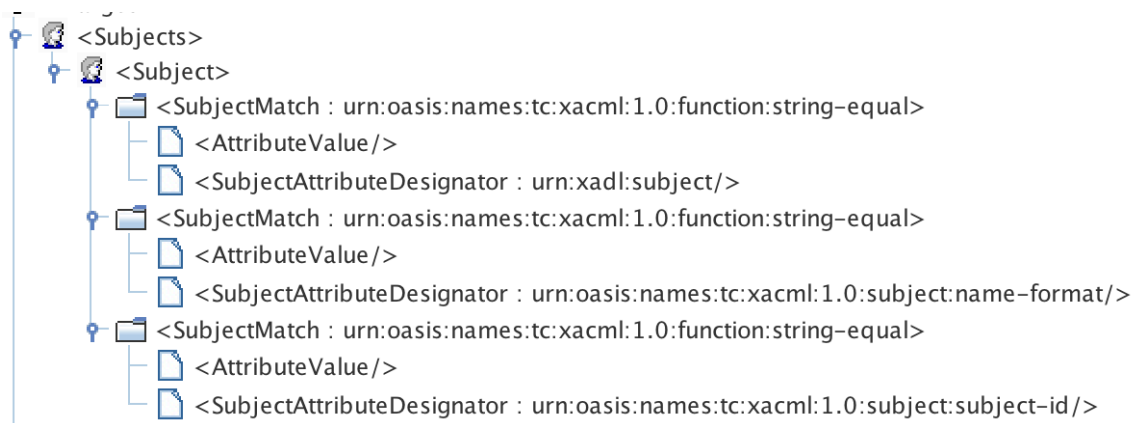
Gambar 4.9 Detail Isian Elemen *Actions First Responder*

Perancangan elemen *environment* pada *user first responder* ini bertujuan untuk menentukan kondisi lingkungan saat *request* dilakukan dan berfungsi mengumpulkan informasi mengenai konteks akses yang dapat digunakan dalam membuat keputusan akses (Sandhu, 2010). Dimulai dengan menentukan nilai *environment match* yang ke-1 yang diberi nilai *function: string-equal*, *attribute value* type data: *string* dan nilai *action: enableRole*. *Environment attribute designator* diberi nilai *subject: authn locality: ip address* type data: *string* serta *issuer* diisi dengan *192.168.0.107*, *must be present* diberi nilai *true*. *Environment match* yang ke-2 menentukan nilai *environment match* diberi nilai *function: string-equal*, *attribute value* type data: *string* dan nilai *action: enableRole*. Selanjutnya menentukan nilai *environment attribute designator* yang *attributeId*nya diisi dengan nilai *subject: authentication time* type data: *string* serta *issuer* diisi dengan “24” yang artinya waktu akses tidak dibatasi, serta *must be present* diberi nilai *true*. *Environment match* yang ke-3 yaitu menentukan nilai *environment match* diberi nilai *function: string-equal*, *attribute value* type data: *string* dan nilai *action: enableRole*. *Environment attribute designator*, *attributeId* diberi nilai *subject: key info* sebagai *mac address* dan type data: *string* serta nilai *issuer* diisi dengan *c4:b3:01:ba:5f:79* nilai *must be present* adalah *true*. Gambar 4.10 merupakan detail isian elemen *environment first responder*.



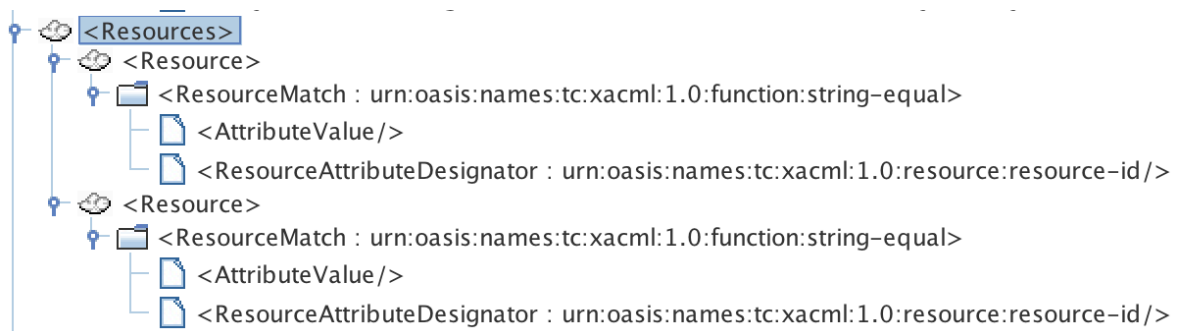
Gambar 4.10 Detail Isian Elemen *Environment first responder*

Penjelasan selanjutnya adalah penjelasan tentang rancangan struktur *policy* yang ada pada *user investigator*. Gambar 4.11 menjelaskan tentang bagaimana isian *target* elemen *subject investigator*, sebagaimana yang dijelaskan pada bagian sebelumnya elemen ini berisi nilai atribut yang dimana nilai atribut tersebut mengandung informasi yang disematkan pada *user investigator*, pada *subject match* yang ke- 1 diberi nilai *string-equal* dan nilai *attribute value type data:string*, *subject attribute designator*, *attributeId* diberi nilai *subject: subject*, *type data: string* serta *issuer* diisi dengan nama *investigator* yang menjadi jabatan *user*. pada *subject match* yang ke- 2 diberi nilai *string-equal* dan nilai *attribute value type data:string*, *subject attribute designator attributeId subject: name format type data: string* serta *issuer* diberi nama *santoso* merupakan nama *user*. *Subject match* yang ke- 3 diberi nilai *function: string-equal* dan *attribute value type data: string* dan *value* diberi nilai *assign user*. *Subject attribute designator* diisi dengan nilai *attributeId: subject-id type data: string* serta *issuer* diisi dengan *santoso123* merupakan *password* pada *user investigator*. Gambar 4.11 merupakan elemen *subject investigator*.



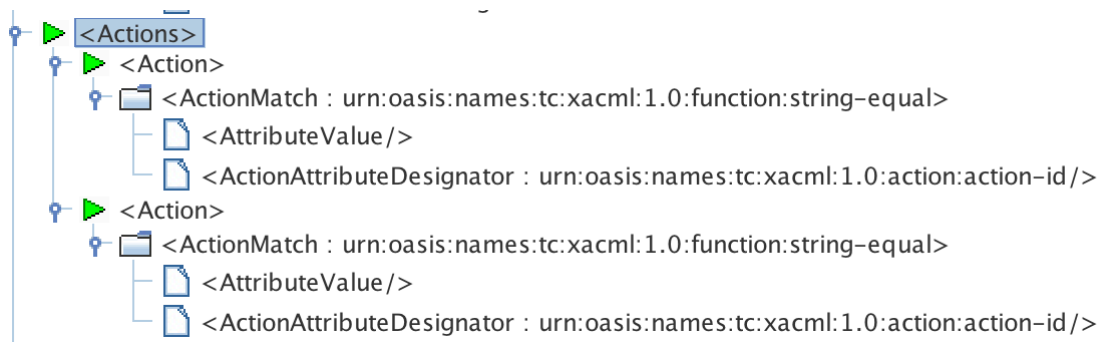
Gambar 4.11 Detail Isian Elemen *Subject Investigator*

Bagian selanjutnya yaitu merupakan proses mengisi kebutuhan elemen *resource* yang menjadi atribut pada *resource user investigator* yang bertujuan untuk menentukan *resource* apa saja yang dapat diakses (Hu et al., 2014) oleh *user investigator* saat menangani barang bukti digital pada LPBD. Diawali dengan menentukan nilai *resource match* yang ke-1 diberi nilai *function: string-equal*, *attribute value typedata: string* dan *value* diberi nama *download file*. *Resource attribute designator* mempunyai *attributeId* diberi nilai *resourceId* *type data: string* serta *issuer* diberi nama *download digital evidence*. Pada *resource match* yang ke-2 diberi nilai *function: string-equal*, *attribute value type data: string* dan *value* diberi nama *complete the data*. *Resource attribute designator* mempunyai *attributeId* diberi nilai *resourceId* *type data: string* serta *issuer* diberi nama *complete the data coc*. Gambar 4.12 adalah detail isian elemen *resource investigator*.



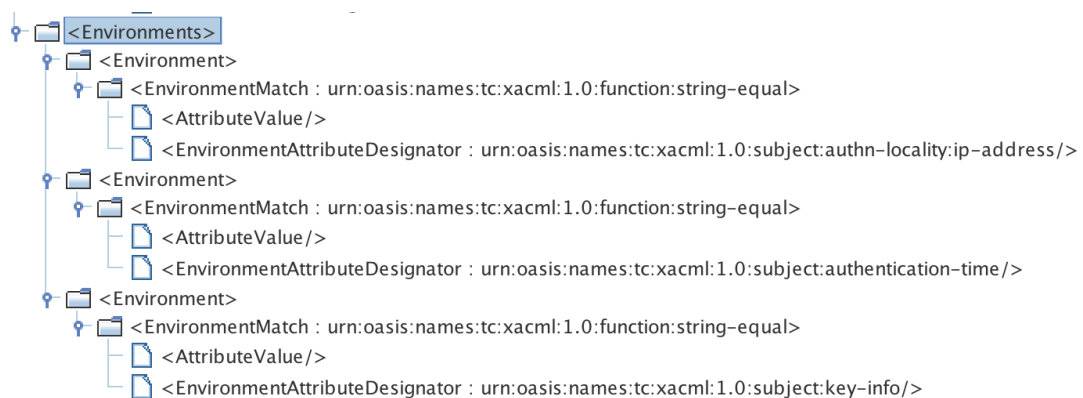
Gambar 4.12 Detail Isian Elemen *Resource Investiigator*

Bagian berikutnya yaitu merancang elemen *actions* yang bertujuan untuk menentukan operasi yang akan dilakukan pada *resource* yang diberikan pada *investigator* sebagai orang yang kedua yang menangani barang bukti digital setelah *first responder* sebagai yang pertama kali menangani bukti digital pada LPBD (Hu et al., 2014). Diawali dengan menentukan nilai *action match* diberi nilai *function; string-equal*, *form attribute value type data: string* dan *value* diberi nama *download* dan *action attribute designator* *attributeId* diberi nilai *actionId* *type data: string* serta *issuer* diberi nama *download file*. Elemen *actions* yang ke-2 menentukan nilai *action match* diberi nilai *function; string-equal* *attribute value type data: string* dan *value* diberi nama *complete data* serta *action attribute designator* mempunyai *attributeId* diberi nilai *actionId* *type data: string* serta *issuer* diberi nama *complete data coc*. Gambar 4.13 merupakan detail isian elemen *actions investigator*.



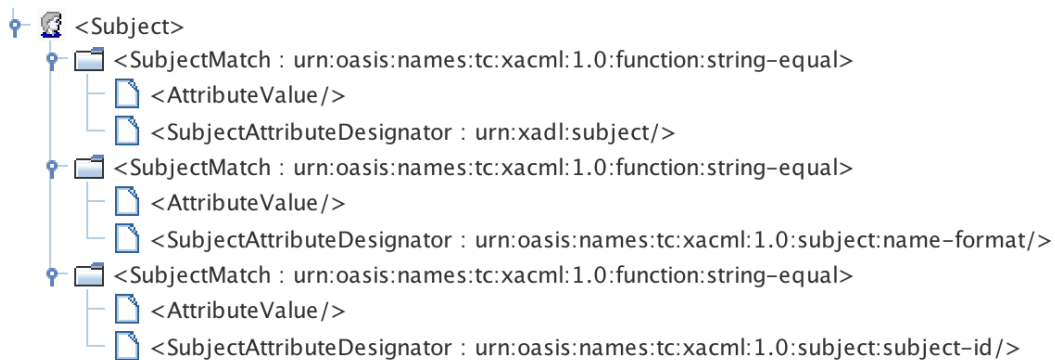
Gambar 4.13 Detail Isian Elemen *Action Investigator*

Perancangan elemen *environment user investigator* bertujuan untuk menentukan kondisi lingkungan saat *request* dilakukan (Sandhu, 2010) oleh investigator, elemen *environment* ini berperan sebagai yang mengumpulkan informasi mengenai konteks akses yang dapat digunakan dalam membuat keputusan akses. Diawali dengan menentukan nilai *environment match* yang ke- 1 diberi nilai *function: string-equal*, *attribute value type data:string* dan nilai *action: enableRole*. *Environment attribute designator* diberi nilai *subject: authn locality: ip address* dan *type data: string* serta *issuer* diisi dengan *192.168.0.108 must be present* adalah *true*. *Environment match* yang ke- 2 menentukan nilai *environment match* diberi nilai *function: string-equal*, *attribute value type data: string* dan nilai *action: enableRole*. *Environment attribute designator* memiliki *attributeId* diberi nilai *subject: authentication time* dan *type data: string* serta *issuer* diberi nama “24” yang artinya waktu akses tidak dibatasi, *must be present* adalah *true*. *Environment match* yang ke- 3 menentukan nilai *environment match* diberi nilai *function: string-equal*, *attribute value type data: string* dan nilai *action: enableRole*. *Environment attribute designator* memiliki *attributeId* diberi nilai *subject: key info* sebagai *mac address* dan *type data: string* serta nilai *issuer* diisi dengan *e4:ce:8f:19:c7:7a* dan *must be present* adalah *true*. Gambar 4.14 detail isian elemen *environment investigator*.



Gambar 4.14 Detail Isian Elemen *Environment Investigator*

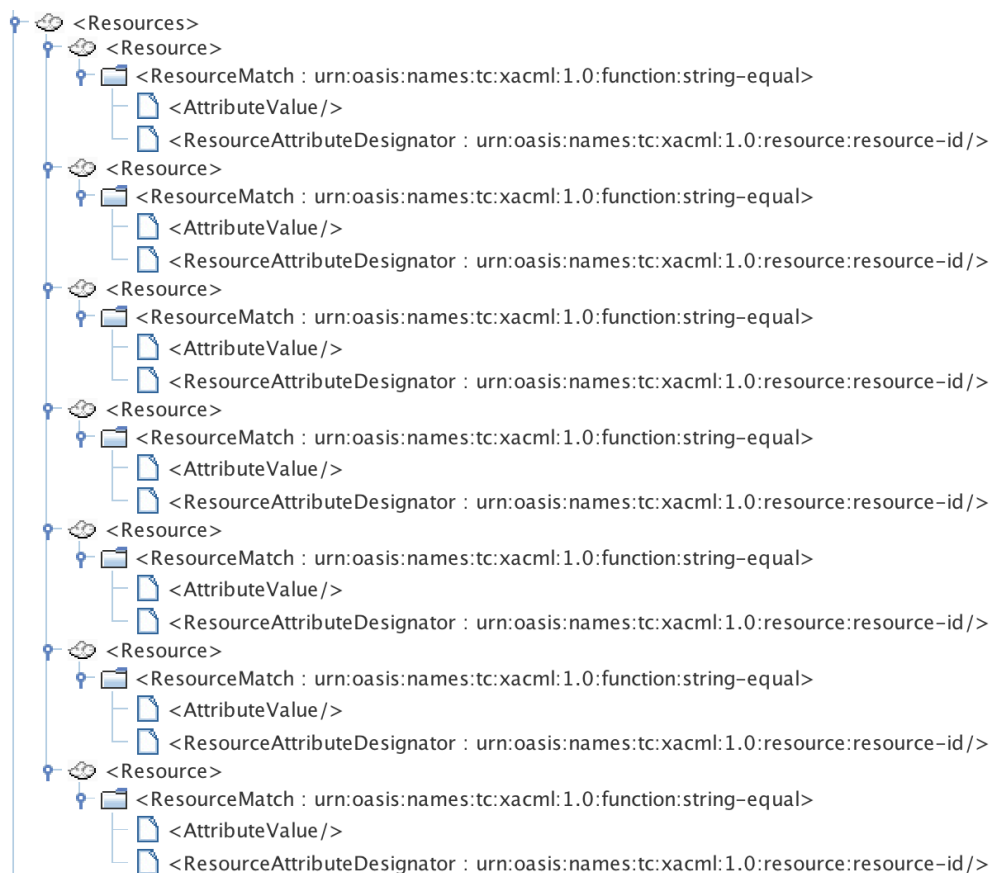
Penjelasan selanjutnya yaitu menjelaskan tentang rancangan struktur *policy* yang ada pada *user officer*. Gambar 4.15 menjelaskan bahwa pada bagian ini adalah langkah pembuatan *subject user officer*, diawali dengan menentukan *target* dengan mengisi nilai atribut yang ada pada *elemen subject*, pada *subject match* yang ke- 1 diberi nilai *string-equal attribute value type data: string* dan *value* diberi nilai *assign user*. *Subject attribute designator* memiliki *attributeId* diberi nilai *subject: subject type data: string* serta pada *issuer* diisi dengan nama *officer* yang merupakan jabatan *user*. *Subject match* yang ke- 2 diberi nilai *string-equal, attribute value type data:string* dan *value* diberi nilai *assign user*. *Subject attribute designator* memiliki *attributeId* diberi nilai *subject: name format type data: string* serta *issuer* diberi nama *dadang* yang menjadi *username* pada jabatan *officer*. *Subject match* yang ke- 3 diberi nilai *function: string-equal, attribute value type data: string* dan *value* diberi nilai *assign user*. *Subject attribute designator* memiliki *attributId: subject-id type data: string* serta *issuer* diberi nama *dadang123* yang menjadi *password user*. Gambar 4.15 merupakan detail isian elemen *subject officer*.



Gambar 4.15 Detail Isian Elemen *Subject Officer*

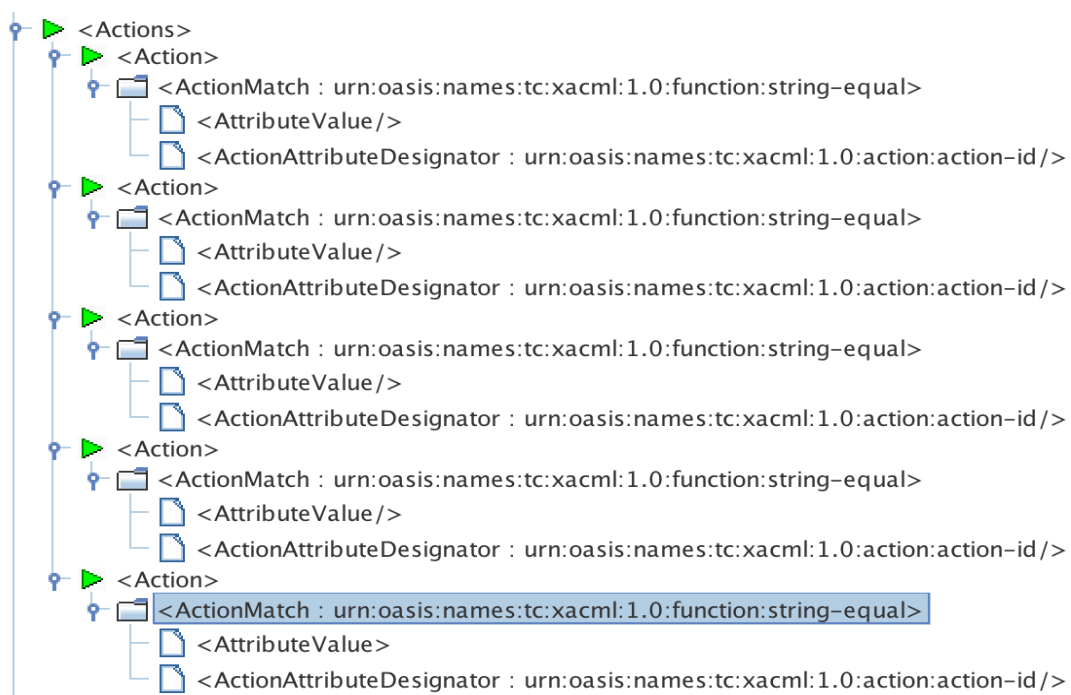
Langkah selanjutnya yaitu merancang elemen *resource user officer* yang bertujuan untuk menentukan *resource* apa saja yang dapat diakses (Sandhu, 2010) oleh *user officer* saat melakukan *request*. Diawali dengan menentukan nilai *resource match* yang ke- 1 diberi nilai *function: string-equal, attribute value type data: string* dan *value* diberi nama *delete file digital evidence*. *Resource attribute designator* mempunyai *attributeId: resourceId type data: string* serta *issuer* diberi nama *delete digital evidence*. Pada *resource match* yang ke- 2 diberi nilai *function: string-equal, attribute value type data: string* dan *value* diberi nama *change password*. *Resource attribute designator* memiliki *attributeId: resourceId type data: string* serta *issuer* diberi nama *change password user*. *Resource match* yang ke- 3 diisi dengan nilai *function: string-equal attribute value type data: string* serta *value* diberi nama

validate file digital evidence. *Resource attribute designator* mempunyai *attributeId*: *resourceId* *type data*: *string* serta *issuer* diberi nama *validate digital evidence*. *Resource match* yang ke- 4 diberi nilai *function*: *string-equal*, *attribute value type data*: *string* serta *value* diberi nama *validate case*. *Resource attribute designator* mempunyai *attributeId*: *resourceId* *type data*: *string* serta *issuer* diberi nama *validate case status*. Pada *resource match* yang ke- 5 diberi nilai *function*: *string-equal*, *attribute value type data*: *string* dan *value* diberi nama *download file form coc*. *Resource attribute designator* memiliki *attributeId*: *resourceId* *type data*: *string* serta *issuer* diberi nama *download form coc*. *Resource match* yang ke- 6 diberi nilai *function*: *string-equal*, *attribute value type data*: *string* dan *value* diberi nama *change code*. *Resource attribute designator* memiliki *attributeId*: *resourceId* *type data*: *string* serta *issuer* diberi nama *change code signature*. *Resource match* bagian ke- 7 diberi nilai *function*: *string-equal*, *attribute value type data*: *string* dan *value* diberi nama *validate data*. *Resource attribute designator* memiliki *attributeId*: *resourceId* *type data*: *string* serta *issuer* diberi nama *validate data coc*. Gambar 4.16 adalah detail isian elemen *resource officer*.



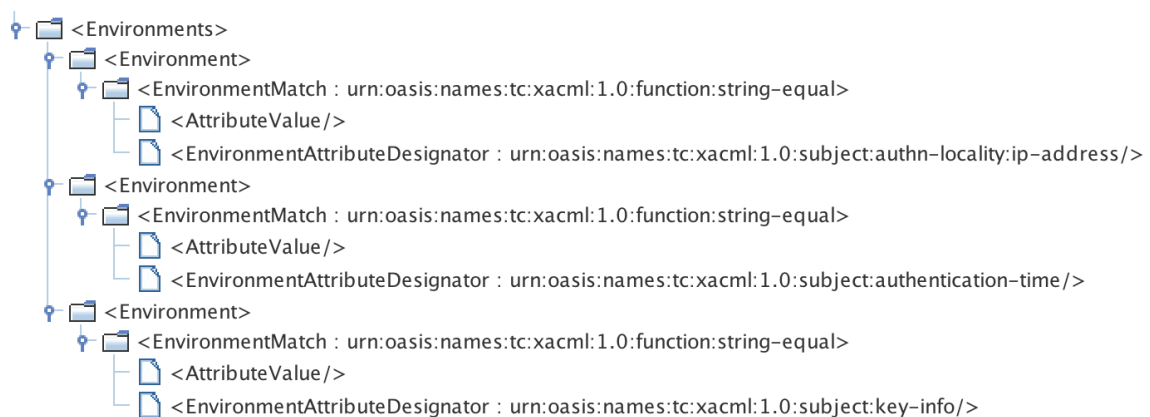
Gambar 4.16 Detail Isian Elemen *Resource Officer*

Tahapan selanjutnya yaitu merancang elemen *actions* yang bertujuan untuk menentukan *actions* yang dilakukan *officer* serta sebagai penentu operasi yang akan dilakukan pada *resource* yang dapat diakses (Sandhu, 2010). Diawali dengan menentukan nilai *action match* diberi nilai *function; string-equal*, *attribute value type data: string* dan *value* diberi nama *delete*. *Action attribute designator* mempunyai *attributeId: actionId type data: string* serta *issuer* diberi nama *delete file*. Elemen *actions* yang ke- 2, menentukan nilai *action match* diberi nilai *function; string-equal*, *attribute value type data: string* dan *value* diberi nama *change password*. *Action attribute designator* memiliki *attributeId: actionId type data: string* serta *issuer* diberi nama *change password user*. Elemen *actions* yang ke- 3 menentukan nilai *action match* diberi nilai *function: string-equal*, *attribute value type data: string* dan *value* diberi nama *validate*. *Action attribute designator* memiliki *attributeId: actionId type data: string* serta *issuer* diberi nama *validate file, status, data*. Elemen *actions* yang ke- 4 menentukan nilai *action match* diberi nilai *function; string-equal*, *attribute value type data: string* dan *value* diberi nama *download*. *Action attribute designator* memiliki *attributeId: actionId type data: string* serta *issuer* diberi nama *download form*. Elemen *actions* yang ke- 5 menentukan nilai *action match* yang diberi nilai *function; string-equal*, *attribute value type data: string* serta *value* diberi nama *change*. *Action attribute designator* memiliki *attributeId: actionId type data: string* serta *issuer* diberi nama *change code*. Gambar 4.17 adalah detail isian elemen *actions officer*.



Gambar 4.17 Detail Isian Elemen *Action Officer*

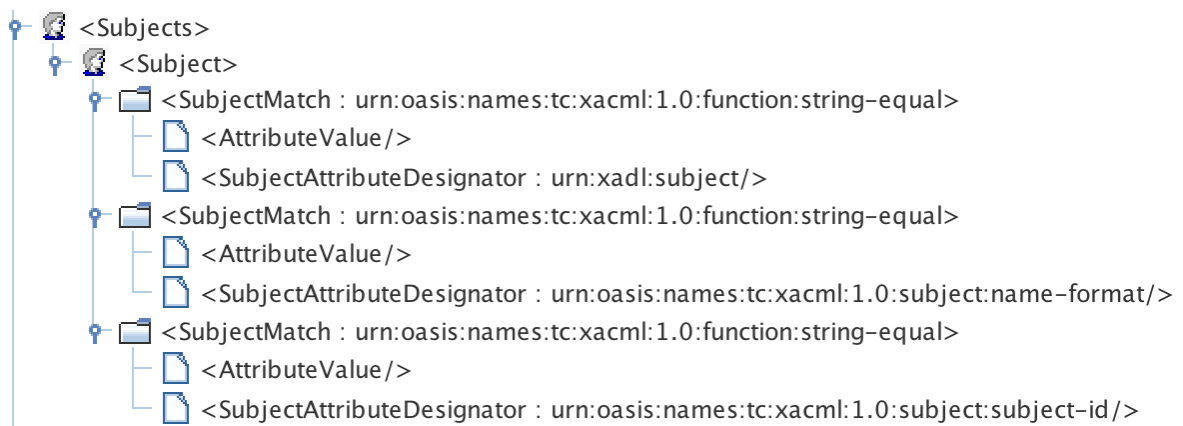
Tahapan berikutnya yaitu merancang elemen *environment* pada *user officer* yang bertujuan untuk menentukan kondisi lingkungan saat *request* akses dilakukan (Sandhu, 2010) oleh *officer* serta berfungsi sebagai mengumpulkan informasi mengenai konteks akses yang dapat digunakan dalam membuat keputusan akses. Langkah awal perancangan *elemen* ini diawali dengan menentukan nilai *environment match* yang ke- 1 diberi nilai *function: string-equal*, *attribute value type data: string* dan nilai *action: enableRole*. *Environment attribute designator* diberi nilai *subject: authn locality: ip address type data: string* serta *issuer* diisi dengan *192.168.1.1* serta *must be present* adalah *true*. *Environment match* yang ke- 2 menentukan nilai *environment match* diberi nilai *function: string-equal*, *attribute value type data: string* dan nilai *action: enableRole*. *Environment attribute designator* memiliki *attributeId: subject: authentication time type data: string* serta *issuer* diisi dengan “24” yang artinya waktu akses tidak dibatasi, dan *must be present* adalah *true*. *Environment match* yang ke- 3, menentukan nilai *environment match* diberi nilai *function: string-equal*, *attribute value type data: string* dan nilai *action: enableRole*. *Environment attribute designator* memiliki *attributeId: subject: key info* yaitu *mac address, type data: string* serta nilai *issuer* diisi dengan *Fe80::4c2c:f62a:de:a57c%11* dan *must be present* adalah *true*. Gambar 4.18 adalah detail isian elemen *environment officer*.



Gambar 4.18 Detail Isian Elemen *Environment Officer*

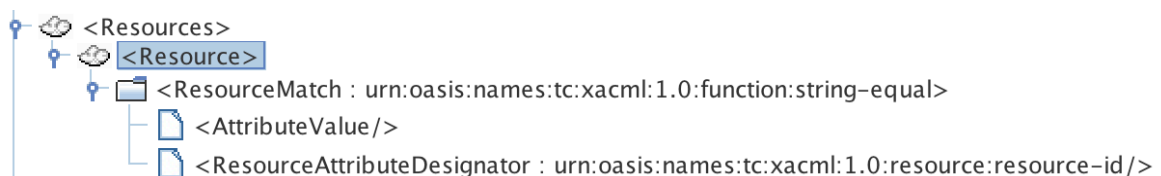
Penjelasan selanjutnya yaitu menjelaskan rancangan *policy* yang ada pada *user lawyer*. Gambar 4.19 menjelaskan bahwa pada bagian ini adalah menjelaskan tentang rancangan *policy user lawyer* merupakan ekspresi logika saat *user lawyer* melakukan *request*. Diawali dengan menentukan *target* dengan mengisi nilai atribut yang ada pada *elemen subject*, pada *subject match* yang ke- 1 diisi dengan nilai *string-equal* dan nilai *attribute value type data: string* dan *value* diberi nilai *assign user*. *Subject attribute*

designator memiliki *attributeId*: *subject*: *subject* *type data*: *string* dan *issuer* diberi nama *lawyer* yaitu jabatan *user*. Pada *subject match* yang ke- 2 diberi nilai *function*: *string-equal*, *attribute value type data*: *string* dan *value* diberi nilai *assign user*. *Subject attribute designator* memiliki *attributeId*: *subject*: *name format* *type data*: *string* serta *issuer* diberi nama *hotman* yang menjadi nama *user*. *Subject match* yang ke- 3 diberi nilai *function*: *string-equal*, *attribute value type data*: *string* dan *value* diberi nilai *assign user*. *Subject attribute designator* memiliki *attributeId*: *subject*: *subjectId* *type data*: *string* serta *issuer* diberi nama *hotman123* yang menjadi password *user*. Gambar 4.19 adalah detail isian elemen *subject lawyer*.



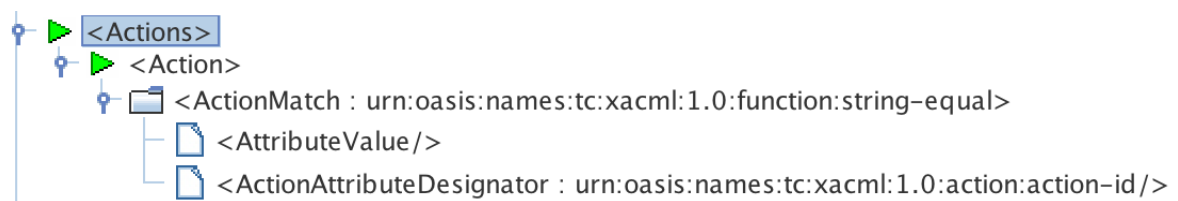
Gambar 4.19 Detail Isian Elemen *Subject Lawyer*

Tahapan selanjutnya yaitu merancang elemen *resource user lawyer* yang bertujuan untuk menentukan kebijakan *resource* yang dapat diakses oleh *user lawyer*. Langkah pertama yaitu dengan menentukan nilai *resource match* diberi nilai *function*: *string-equal*, *attribute value type data*: *string* dan *value* diberi nama *download form*. *Resource attribute designator* memiliki *attributeId*: *resourceId* *type data*: *string* serta *issuer* diberi nama *download form coc*. Gambar 4.20 adalah isian elemen *resource lawyer*.



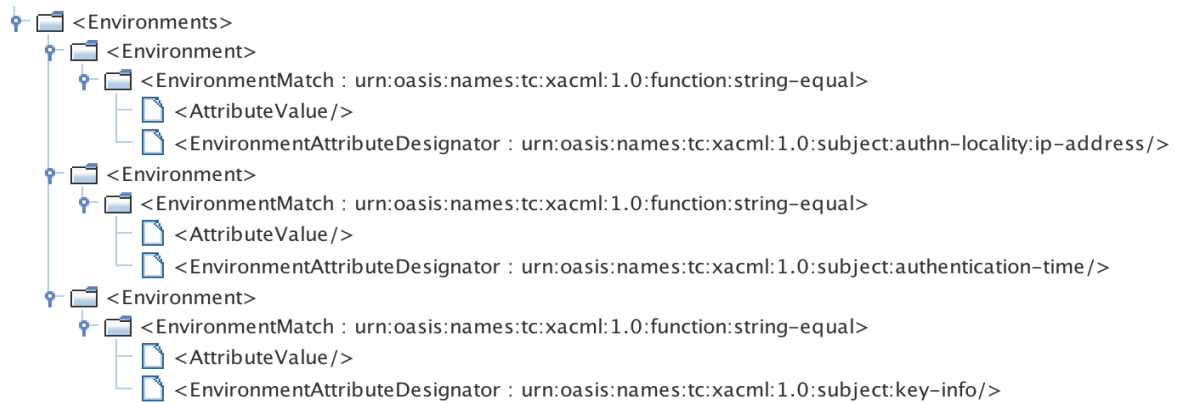
Gambar 4.20 Detail Isian Elemen *Resource Lawyer*

Tahapan berikutnya merupakan rancangan elemen *actions user lawyer* yang bertujuan untuk menentukan *actions* yang dapat dilakukan saat melakukan *request* serta sebagai penentu operasi yang akan dilakukan pada *resource*. Langkah yang dilakukan yaitu menentukan nilai *action match* yang diberi nilai *function: string-equal, attribute value type data: string* dan *value* diberi nama *download*. *Action attribute designator* memiliki *attributeId: actionId type data: string* serta *issuer* diberi nama *download form*. Gambar 4.21 adalah detail isian elemen *action lawyer*.



Gambar 4.21 Detail Isian Elemen *Actions Lawyer*

Perancangan elemen *environment* pada *user lawyer* ini bertujuan untuk menentukan kondisi lingkungan ketika *lawyer* melakukan permintaan akses pada LPBD (Sandhu, 2010). Elemen *environment* juga berperan sebagai yang mengumpulkan informasi mengenai konteks akses yang dapat digunakan dalam membuat keputusan akses. Diawali dengan menentukan nilai *environment match* yang ke- 1 diberi nilai *function: string-equal, attribute value type data: string* dan nilai *action: enableRole*. *Environment attribute designator* memiliki *attributeId: subject: authn locality: ip address type data: string* serta *issuer* diisi dengan *192.168.0.106, must be present* adalah *true*. *Environment match* yang ke- 2 menentukan nilai *environment match* diberi nilai *function: string-equal, attribute value type data: string* dan *action: enableRole*. *Environment attribute designator* memiliki *attributeIdnya: subject: authentication time type data: string* serta *issuer* diisi dengan “09.00-15.00” yang artinya bahwa waktu akses yang diberikan pada *lawyer* hanya pada waktu yang telah dituliskan tersebut karena *lawyer* bukan merupakan petugas yang diberi wewenang untuk menangani bukti digital yang ada pada LPBD, serta *must be present* adalah *true*. *Environment match* yang ke- 3 yaitu menentukan nilai *environment match* diberi nilai *function: string-equal, attribute value type data: string* dan nilai *action: enableRole*. *Environment attribute designator* memiliki *attributeId: subject: key info* yaitu *mac address type data: string* serta nilai *issuer* diisi dengan *d5:6d:7e:19:c2:9c* dan *must be present* adalah *true*. Gambar 4.22 merupakan detail isian elemen *environment user lawyer*.



Gambar 4.22 Detail Isian Elemen *Environment Lawyer*

4.3 Output XACML Policy

Pada subbab ini akan menjelaskan bagaimana keluaran XACML *policy* yang telah dirancang seperti penjelasan pada bab sebelumnya. XACML *policy* ini merupakan struktur *policy* yang sesuai dengan perancangan awal dan akan berfungsi sebagai aturan *policy* pada sistem lemari penyimpanan bukti digital. *Output* hasil rancangan XACML *policy* yang pertama dijelaskan yaitu *target* dari *root* elemen yaitu elemen *policy* sebagaimana yang terlihat pada gambar 4.23.

```

- <Policy PolicyId="Access_Control_Policy_LPBD" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
  - <Target>
    - <Subject>
      - <Subject>
        - <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
          <SubjectAttributeDesignator AttributeId="urn:xadl:subject" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="First Responder" MustBePresent="true"/>
        </SubjectMatch>
        - <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
          <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-format" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="fadlypanende" MustBePresent="true"/>
        </SubjectMatch>
        - <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
          <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="fadly123" MustBePresent="true"/>
        </SubjectMatch>
      </Subject>
    </Subject>
    - <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
      <SubjectAttributeDesignator AttributeId="urn:xadl:subject" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Investigator" MustBePresent="true"/>
    </SubjectMatch>
    - <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
      <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-format" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="santoso" MustBePresent="true"/>
    </SubjectMatch>
    - <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
      <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="santoso123" MustBePresent="true"/>
    </SubjectMatch>
    - <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
      <SubjectAttributeDesignator AttributeId="urn:xadl:subject" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Officer" MustBePresent="true"/>
    </SubjectMatch>
    - <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
      <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-format" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="dadang" MustBePresent="true"/>
    </SubjectMatch>
    - <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>

```

Gambar 4.23 Sample Output XACML Root Elemen

Gambar 4.23 menjelaskan bahwa hasil *output* XACML *policy* bagian ini merupakan *sample* dari keseluruhan jumlah elemen *subject* maupun *resource*. Output XACML *policy* yang telah dibuat berupa tahapan awal pada *target root* elemen *policy* dimana jumlah *subject*

sebanyak 4 buah, dan jumlah *resource* sebanyak 13 buah yang artinya bahwa hanya ada 4 *user* yang berhak melakukan akses pada LPBD dan masing-masing dari *user* tersebut adalah *first responder*, *investigator*, *officer*, dan *lawyer* serta berhak mengakses *resource* yang ada pada LPBD sesuai dengan kebijakan *access* yang telah diberikan. *Resource* yang akan di *access* yaitu *upload file digital evidence*, *create new cabinet*, *create new rack*, *create new bag*, *delete file digital evidence*, *change password user*, *validate file digital evidence*, *validate status case*, *download file form coc*, *change code signature*, *validate data coc*, *download file digital evidence cabinet*, serta *input data case coc*.

4.3.1 Output XACML Policy Elemen Subject

Output rancangan XACML *policy* pada elemen *subject* ini merupakan hasil dari perancangan yang sudah dijelaskan sebelumnya proses ini merupakan keluaran XACML *policy* yang sangat menentukan bagaimana mengkombinasikannya dengan bahasa pemrograman yang akan membaca keluaran XACML *policy* ini selanjutnya,

1. Output Elemen Subject First Responder

Output XACML *Policy* pada elemen *subject first responder* ini merupakan bagian yang menjelaskan bahwa isi dari elemen *subject* ini berupa identitas *user* diantaranya yaitu *jabatan*, *nama* dan *userid*, ketiga atribut yang digunakan pada elemen *subject* ini juga menjadi kebijakan pada *user* yang akan melakukan *request* pada LPBD. Yang artinya bahwa seseorang yang berhak masuk pada sistem harus memenuhi kriteria *username: fadlypanende* dan *password: fadly123* adalah seseorang yang mempunyai jabatan sebagai *first responder* pada LPBD, sebagaimana yang terlihat pada gambar 4.24.

```

- <Rule Effect="Permit" RuleId="Rule1: First Responder">
- <Target>
- <Subjects>
- <Subject>
- <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
- <Attribute Value DataTypeId="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</Attribute Value>
- <SubjectAttributeDesignator AttributeId="urn:xadl:subject" DataTypeId="http://www.w3.org/2001/XMLSchema#string" Issuer="First Responder" MustBePresent="true"/>
- <SubjectMatch>
- <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
- <Attribute Value DataTypeId="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</Attribute Value>
- <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-format" DataTypeId="http://www.w3.org/2001/XMLSchema#string" Issuer="fadlypanende"
MustBePresent="true"/>
- <SubjectMatch>
- <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
- <Attribute Value DataTypeId="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</Attribute Value>
- <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataTypeId="http://www.w3.org/2001/XMLSchema#string" Issuer="fadly123"
MustBePresent="true"/>
- <SubjectMatch>
- <Subject>
- </Subjects>

```

Gambar 4.24 Output Subject First Responder

2. Output Elemen Subject Investigator

Bagian ini merupakan penjelasan tentang bagaimana hasil dari *output XACML Policy* pada elemen *subject investigator*. Isi dari elemen *subject* ini berupa identitas *user* diantaranya yaitu *jabatan*, *nama* dan *userid*, ketiga atribut yang digunakan pada *elemen subject* ini juga menjadi kebijakan pada *user* yang akan melakukan *request* pada LPBD. Yang artinya bahwa seseorang yang berhak masuk pada sistem harus memenuhi kriteria *username: santoso* dan *password: santoso123* adalah seseorang yang mempunyai jabatan sebagai *investigator* pada LPBD. Sebagaimana yang terlihat pada gambar 4.25.

```
-<Subjects>
-<Subject>
-<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
  <SubjectAttributeDesignator AttributeId="urn:xadl:subject" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Investigator" MustBePresent="true"/>
</SubjectMatch>
-<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
  <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-format" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="santoso"
  MustBePresent="true"/>
</SubjectMatch>
-<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
  <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="santoso123"
  MustBePresent="true"/>
</SubjectMatch>
</Subject>
</Subjects>
```

Gambar 4.25 Output Subject Investigator

3. Output Elemen Subject Officer

Output XACML Policy pada elemen *subject investigator*. Isi dari elemen *subject* ini berupa identitas *user* diantaranya yaitu *jabatan*, *nama* dan *userid*, ketiga atribut yang digunakan pada elemen *subject* ini juga menjadi kebijakan pada *user* yang akan melakukan *request* pada LPBD. Yang artinya bahwa seseorang yang berhak masuk pada sistem harus memenuhi kriteria *username: dadang* dan *password: dadang123* adalah seseorang yang mempunyai jabatan sebagai *officer* pada LPBD, sebagaimana yang terlihat pada gambar 4.26.

```
-<Subjects>
-<Subject>
-<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
  <SubjectAttributeDesignator AttributeId="urn:xadl:subject" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Officer" MustBePresent="true"/>
</SubjectMatch>
-<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
  <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-format" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="dadang"
  MustBePresent="true"/>
</SubjectMatch>
-<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</AttributeValue>
  <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="dadang123"
  MustBePresent="true"/>
</SubjectMatch>
</Subject>
</Subjects>
```

Gambar 4.26 Output Elemen Subject officer

4. Output Elemen *Subject Lawyer*

Output XACML Policy pada elemen *subject investigator*. Isi dari elemen *subject* ini berupa identitas *user* diantaranya yaitu *jabatan*, *nama* dan *userid*, ketiga atribut yang digunakan pada elemen *subject* ini juga menjadi kebijakan pada *user* yang akan melakukan *request* pada LPBD. Yang artinya bahwa seseorang yang berhak masuk pada sistem harus memenuhi kriteria *username: hotman* dan *password: hotman123* adalah seseorang yang mempunyai jabatan sebagai *lawyer* pada LPBD, sebagaimana yang terlihat pada gambar 4.27.

```
-<Subjects>
-<Subject>
-<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</Attribute Value>
  <SubjectAttributeDesignator AttributeId="urn:xadl:subject" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Lawyer" MustBePresent="true"/>
</SubjectMatch>
-<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</Attribute Value>
  <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-format" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="hotman" MustBePresent="true"/>
</SubjectMatch>
-<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac:assignUser</Attribute Value>
  <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="hotman123" MustBePresent="true"/>
</SubjectMatch>
</Subject>
</Subjects>
```

Gambar 4.27 Output Elemen *Subject Lawyer*

4.3.2 Output XACML Policy Elemen *Resource*

Berbeda dengan *output* yang dijelaskan sebelumnya, pada bagian ini akan dijeaskan bagaimana *output* yang ada pada elemen *resource* atribut yang ada pada elemen *resource* ini merupakan atribut yang berkaitan dengan kebijakan apa saja yang berhak dioperasikan ketika telah berhasil melakukan *login* pada LPBD.

1. Output Elemen *Resource First Responder*

Pada *output* elemen *resource first responder* ini menjelaskan tentang kebijakan apa saja yang telah diberikan pada *user first responder* untuk mengakses *resource* atribut yang diberikan sesuai wewenang pekerjaan sebagai *first responder*. Sebagaimana yang terlihat pada rancangan *policy statement* sebelumnya bahwa ada 5 atribut yang diberikan sebagai hak akses *resource* pada *first responder* yaitu berupa *upload file digital evidence*, *create new cabinet*, *create new rack*, *create new bag*, *input data case coc* yang artinya adalah seseorang yang berwenang melakukan aktifitas *upload file digital evidence*, *create new cabinet*, *create new rack*, *create new*, *input data case coc bag* yaitu seseorang yang memiliki jabatan sebagai *first responder* pada LPBD. Sebagaimana yang terlihat pada gambar 4.28.


```

- <Resources>
- <Resource>
- <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Upload File Digital Evidence</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Upload Digital Evidence"
    MustBePresent="true"/>
  </ResourceMatch>
- </Resource>
- <Resource>
- <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Create New Cabinet</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Create Cabinet"
    MustBePresent="true"/>
  </ResourceMatch>
- </Resource>
- <Resource>
- <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Create New Rack</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Create Rack"
    MustBePresent="true"/>
  </ResourceMatch>
- </Resource>
- <Resource>
- <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Create New Bag</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Create Bag"
    MustBePresent="true"/>
  </ResourceMatch>
- </Resource>
- <Resource>
- <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Input Data Case Coc</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Input Data Coc"
    MustBePresent="true"/>
  </ResourceMatch>
- </Resource>
</Resources>

```

Gambar 4.28 Output Resource First Responder

2. Output Elemen Resource Investigator

Pada bagian ini menjelaskan bagaimana *output XACML policy* pada *resource investigator*, ada 2 atribut yang diberikan pada *resource investigator*, atributnya yaitu *download file digital evidence* dan *complete the data coc* yang artinya bahwa seseorang yang mempunyai wewenang *download file digital evidence* dan *complete the data coc* adalah seseorang yang memiliki jabatan sebagai *investigator* pada LPBD, sebagaimana yang terlihat pada gambar 4.29.

```

- <Resources>
- <Resource>
- <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Download File</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download Digital Evidence"
    MustBePresent="true"/>
  </ResourceMatch>
- </Resource>
- <Resource>
- <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Complete the Data</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Complete The Data Coc"
    MustBePresent="true"/>
  </ResourceMatch>
- </Resource>
</Resources>

```

Gambar 4.29 Output Elemen Resource Investigator

3. Output Elemen Resource Officer

Output resource officer menjelaskan tentang keluaran hasil rancangan *XACML policy* pada *resource officer*. Ada 7 atribut yang disematkan pada *resource officer* atribut yang diberikan yaitu *validate file digital evidence*, *validate file data coc*, *validate status case*, *change code signature*, *download file form coc*, *change password user*, *delete digital evididence*, yang artinya bahwa seseorang yang memiliki wewenang yang melakukan hal yang tertulis diatas

adalah merupakan seseorang yang memiliki jabatan sebagai *officer* pada LPBD. Sebagaimana yang terlihat pada gambar 2.30.

```

-<Resource>
-<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Delete File</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Delete Digital Evidence"
  MustBePresent="true"/>
</ResourceMatch>
</Resource>
-<Resource>
-<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Change Password</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Change Password First
  Responder, Investigator, Lawyer" MustBePresent="true"/>
</ResourceMatch>
</Resource>
-<Resource>
-<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Validate File</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Validate File Digital
  Evidence" MustBePresent="true"/>
</ResourceMatch>
</Resource>
-<Resource>
-<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Validate Status</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Validate Status Case"
  MustBePresent="true"/>
</ResourceMatch>
</Resource>
-<Resource>
-<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Download Form</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download Form Coc"
  MustBePresent="true"/>
</ResourceMatch>
</Resource>
-<Resource>
-<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Change Code</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Change Code Signature"
  MustBePresent="true"/>
</ResourceMatch>
</Resource>

```

Gambar 4.30 Output Elemen *Resource Officer*

4. Output Elemen *Resource Lawyer*

Pada bagian ini menjelaskan tentang bagaimana hasil rancangan dan kebijakan yang diberikan pada *resource lawyer*, ada satu atribut yang diberikan yaitu *download file form coc* yang artinya bahwa seseorang yang memiliki kewenangan hanya melakukan *download file form coc* adalah seseorang yang memiliki jabatan sebagai seorang *lawyer* pada LPBD. Sebagaimana yang terlihat pada gambar 4.31.

```

-<Resources>
-<Resource>
-<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Download Form</AttributeValue>
  <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download Form Coc"
  MustBePresent="true"/>
</ResourceMatch>
</Resource>
</Resources>

```

Gambar 4.31 Output Elemen *Resource Lawyer*

4.3.3 Output XACML Policy Elemen Actions

Bagian ini menjelaskan tentang bagaimana output XACML *policy* yang ada pada elemen *actions* secara keseluruhan yang sudah dirancang sebelumnya.

1. Output Elemen *Actions First Responder*

Output elemen *actions first responder* menjelaskan bahwa ada tiga atribut yang disematkan pada elemen *actions* ini yaitu *upload file*, *create cabinet*, *rack*, *bag*, dan *input* artinya adalah

ketika *user* yang melakukan *request* memenuhi kebijakan yang ada pada *elemen actions* ini maka *user* tersebut akan dikenali sebagai *user first responder* pada LPBD. Sebagaimana yang terlihat pada gambar 4.32.

```

-<Actions>
-<Action>
-<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Upload</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Upload File" MustBePresent="true"/>
</ActionMatch>
</Action>
-<Action>
-<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Create</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Create Cabinet, Rack, Bag" MustBePresent="true"/>
</ActionMatch>
</Action>
-<Action>
-<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Input</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Input Data" MustBePresent="true"/>
</ActionMatch>
</Action>
</Actions>

```

Gambar 4.32 *Output Actions First Responder*

2. *Output Elemen Actions Investigator*

Output elemen actions investigator menjelaskan bahwa hanya ada 2 atribut yang diberikan pada elemen *actions investigator* yaitu *download* dan *complete data coc* artinya adalah ketika *user* yang melakukan *request* memenuhi kebijakan pada elemen *actions* ini, maka *user* tersebut akan dikenali sebagai *user investigator* pada LPBD. Sebagaimana yang terlihat pada gambar 4.33.

```

-<Actions>
-<Action>
-<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Download</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download File" MustBePresent="true"/>
</ActionMatch>
</Action>
-<Action>
-<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Complete Data</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Complete Data Coc" MustBePresent="true"/>
</ActionMatch>
</Action>
</Actions>

```

Gambar 4.33 *Output Actions Investigator*

3. *Output Elemen Actions Officer*

Output elemen actions officer menjelaskan bahwa ada lima atribut yang disematkan pada elemen *actions officer* yaitu, *validate*, *change code*, *download*, *change password*, dan *delete*, artinya adalah ketika *user* yang melakukan *request* memenuhi kebijakan pada elemen *actions* ini, maka *user* tersebut akan dikenali sebagai *user officer* pada LPBD. Sebagaimana yang terlihat pada gambar 4.34.

```

-<Actions>
-<Action>
-<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Delete</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Delete File"
MustBePresent="true"/>
</ActionMatch>
</Action>
-<Action>
-<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Change Password</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Change Password User"
MustBePresent="true"/>
</ActionMatch>
</Action>
-<Action>
-<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Validate</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Validate File, Status, Data"
MustBePresent="true"/>
</ActionMatch>
</Action>
-<Action>
-<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Download</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download Form"
MustBePresent="true"/>
</ActionMatch>
</Action>
-<Action>
-<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Change Code</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Change" MustBePresent="true"/>
</ActionMatch>
</Action>
</Actions>

```

Gambar 4.34 *Output* Elemen *Actions Officer*

4. *Output* Elemen *Actions Lawyer*

Output elemen *actions lawyer* menjelaskan tentang bagaimana *output* hasil perancangan XACML *policy* yang dirancang pada *elemen actions lawyer*, hanya ada satu atribut yang diberikan pada *elemen actions lawyer* yaitu *download* artinya adalah ketika *user* yang melakukan *request* dapat memenuhi kebijakan pada elemen *actins* ini, maka *user* tersebut akan dikenali sebagai *user* pada LPBD. Sebagaimana yang terlihat pada gambar 4.35.

```

-<Actions>
-<Action>
-<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Download</AttributeValue>
<ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download Form"
MustBePresent="true"/>
</ActionMatch>
</Action>
</Actions>

```

Gambar 4.35 *Output* Elemen *Ations Lawyer*

4.3.4 *Output* XACML *Policy* Elemen *Environment*

Pada bagian ini menjelaskan tentang bagaimana *output* XACML *policy* pada elemen *environment* yang telah dirancang sebelumnya.

1. *Output* Elemen *Environment First Responder*

Output pada elemen *environment first responder* ini menjelaskan bahwa ada tiga atribut yang disematkan pada elemen *environment first responder* yaitu *ip address=192.168.0.107*, *authentication time=24*, dan *key info* sebagai *mac address= c4:b3:01:ba:5f:79* artinya adalah bahwa *resource* yang memiliki *ip address = 192.168.0.107* dan *mac address =*

c4:b3:01:ba:5f:79 dapat diberikan hak akses pada LPBD sebagai aktor *first responder* tanpa batasan waktu akses. Sebagaimana yang terlihat pada gambar 4.36.

```

-<Environments>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</Attribute Value>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authn-locality-ip-address" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="192.168.0.107" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</Attribute Value>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="24" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</Attribute Value>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:key-info" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="c4:b3:01:ba:5f:79" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
</Environments>

```

Gambar 4.36 Output Elemen *Environment First Responder*

2. Output Elemen *Environment Investigator*

Output pada elemen *environment investigator* ini menjelaskan tidak ada perbedaan jumlah atribut dengan elemen *environment first responder* perbedaan hanya terletak pada nilai atribut yang diberikan. Atribut yang disematkan pada *elemen environment investigator* yaitu *ipaddress=192.168.0.108*, *authenticationtime=24* dan *keyinfo* sebagai *macaddress=e4:ce:8f:19:c7:7a* artinya bahwa setiap *resource* yang memiliki *ip address=192.168.0.108* dan *mac address= e4:ce:8f:19:c7:7a* dapat diberikan hak akses pada LPBD sebagai *investigator* tanpa batasan waktu akses. Sebagaimana yang terlihat pada gambar 4.37.

```

-<Environments>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</Attribute Value>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authn-locality-ip-address" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="192.168.0.108" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</Attribute Value>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="24" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</Attribute Value>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:key-info" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="e4:ce:8f:19:c7:7a" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
</Environments>

```

Gambar 4.37 Output *Environment Investigator*

3. Output Elemen *Environment Officer*

Output elemen *environment officer* menjelaskan bahwa sama seperti elemen *first responder* dan *investigator* tidak ada perbedaan secara jumlah atribut hanya saja berbeda pada nilai atribut yang disematkan, atribut yang diberikan pada elemen *environment officer* yaitu *ipaddress= 192.168.1.1*, *authenticationtime=24* dan *keyinfo* sebagai *mac address= Fe80::4c2c:f62a:de:a57c%11* artinya bahwa setiap *resource* yang mempunyai *ip address= 192.168.1.1* dan *mac address= Fe80::4c2c:f62a:de:a57c%11* dapat diberikan hak akses sebagai *officer* tanpa batasan waktu akses. Sebagaimana yang terlihat pada gambar 4.38.

```
-<Environments>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</Attribute Value>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authn-locality:ip-address" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="192.168.1.1" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</Attribute Value>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="24" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Attribute Value DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</Attribute Value>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:key-info" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="Fe80::4c2c:f62a:de:a57c%11" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
</Environments>
```

Gambar 4.38 Output *Environment Officer*

4. Output Elemen *Environment Lawyer*

Pada output elemen *environment lawyer* ini menjelaskan bahwa sama halnya seperti elemen – elemen *environment* yang telah dijelaskan sebelumnya yaitu tidak terdapat perbedaan pada jumlah atribut, hanya saja pada nilai atribut yang diberikan. Atribut yang diberikan pada elemen *environment lawyer* yang dianggap sebagai tamu yang dalam hal ini tidak diberikan wewenang untuk menangani bukti digital yang ada pada LPBD yaitu *ip address= 192.168.0.106* sebagai identitas IP, *authentication time=09.00-15.00*, dan *key info* sebagai identitas *mac address= d5:6d:7e:19:c2:9c* artinya bahwa setiap *resource* yang memiliki *ip address=192.168.0.106* dan *mac address= d5:6d:7e:19:c2:9c* dapat diberikan hak akses sebagai *lawyer* dengan waktu akses yang sudah ditentukan yaitu dimulai dari pukul 09.00 sampai dengan pukul 15.00, waktu akses yang diberikan diasumsikan sebagai jam aktif kerja pada instansi-instansi pada umumnya. Sebagaimana yang terlihat pada gambar 4.39.

```

-<Environments>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</AttributeValue>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authn-locality:ip-address" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="192.168.0.106" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</AttributeValue>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="09.00-15.00" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
-<Environment>
  -<EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</AttributeValue>
    <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:key-info" DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="d5:6d:7e:19:c2:9c" MustBePresent="true"/>
  </EnvironmentMatch>
</Environment>
</Environments>

```

Gambar 4.39 Output Elemen *Environment Lawyer*

4.4 Source Code Pembacaan

Pada tahapan ini yaitu menjelaskan tentang bagaimana *source code* yang dapat membaca struktur XACML yang telah dibuat sebelumnya untuk dapat diaplikasikan menjadi sebuah model halaman *login* untuk aplikasi LPBD. Tabel 4.2 adalah *source code* yang digunakan.

Tabel 4.2 List Source Code

No	Source Code	Keterangan
1	<code>username = sel.userName .ge ()</code>	Menerima masukan dari pengguna berupa username
2	<code>password = self.passwordName.get ()</code>	Menangkap masukan dari pengguna berupa password
3	<code>file = open('rules.xhtml', 'r')</code>	Proses membuka file yang berisi XACML
4	<code>tree = ET.parse(file)</code>	Melakukan <i>parsing file</i> dari biner ke teks
5	<code>oot = tree.getroot ()</code>	Mencari <i>top root</i> (struktur tertinggi) dari struktur xml
6	<code>ip_fr = (socket.gethostbyname (socket.gethostname ()))</code>	Mencari ip komputer
7	<code>mac = get_mac ()</code>	Mencari <i>mac address</i>
8	<code>mzc = str(mac)</code>	Mengkonversi <i>mac address</i> menjadi <i>string</i>
9	<code>rule = root.find (".//{urn:oasis:names:tc:xacml:2.0:policy</code>	Membuka <i>rule</i> (diasumsikan bahwa proses pencarian awal

Tabel 4.2 *List Source Code* (Lanjutan)

No	Source Code	Keterangan
	:schema:os} Rule[@RuleId='Rule1: First Responder']")	<i>username</i> dan <i>password</i> dari rule)
10	subjectq = rule.find (".//{urn:oasis:names:tc:xacml:2.0: policy :schema:os} Subjects")	Mencari <i>subject</i> untuk mencari <i>username</i> dan <i>password</i> pada rule1
11	check_up1 = []	Array untuk menampung nilai dari atribut <i>Issuer</i> pada elemen <i>SubjectAttributeDesignator</i> di <i>Subjects</i>
12	check_ulx = ""	Variabel untuk menampung hasil pencarian <i>username</i> di <i>array</i>
13	check_plx = ""	Variabel untuk menampung hasil pencarian <i>password</i> di <i>array</i>
Perulangan untuk mengeluarkan nilai atribut dari elemen <i>SubjectAttributeDesignator</i>		
14	for rule in subjectq.getchildren(): for rules.getchildren(): check_up1.append(rule.find)	Venampung nilai atribut ke dalam <i>array</i> <i>check_up1</i>
15	try: check_up1.index(username)	Mencari <i>username</i> di dalam <i>array</i>
16	except: check_ulx = "none"	Jika tidak ada di set <i>none</i>
17	else: check_ulx = "available"	Jika ada di set <i>available</i>
18	try: check_up1.index(password)	Mencari <i>username</i> di dalam <i>array</i>
19	except: check_plx = "none"	Jika tidak ada di set <i>none</i>
20	else: check_plx = "available"	Jika ada di set <i>available</i>
21	if check_ulx == "available" and check_plx == "available":	Kondisi jika <i>username</i> dan <i>password</i> ada di <i>rules</i>
22	self.rules = root.find env = self.rules.find env1 = self.rules.find	Kondisi jika <i>username</i> dan <i>Password</i> ada di <i>rules</i>

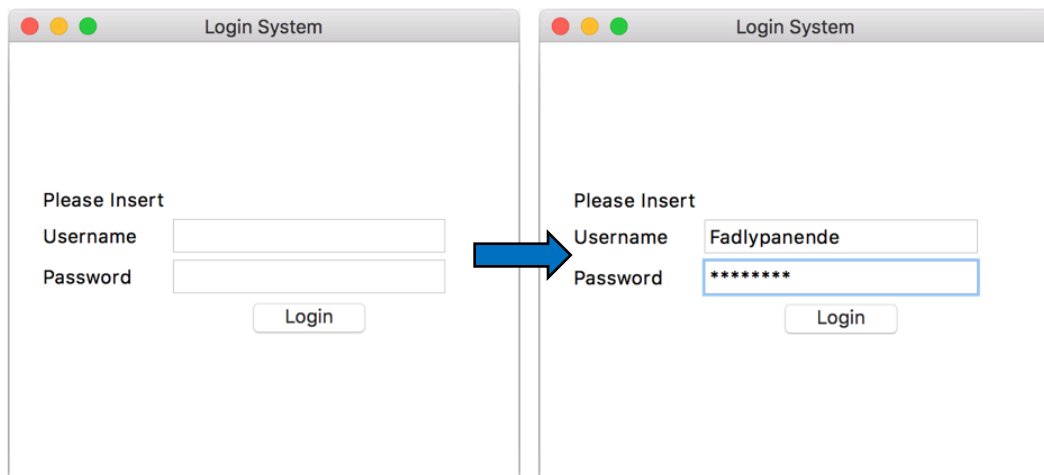
Tabel 4.2 *List Source Code* (Lanjutan)

No	Source Code	Keterangan
23	<code>ip = env.find</code>	Cari IP Address
24	<code>macz = env1.find</code>	Cari Mac Address
25	<code>if ip is not None and macz is not None: tkMessageBox.showinfo("Info", "Welcome LPBD!" + username + "\nYou Logged as First Responder")</code>	Kondisi jika ada IP address dan Mac address
26	<code>else: if ip is None: tkMessageBox.showerror("Info", "Incorrect IP Address!")</code>	Kondisi jika tidak ada IP Address
27	<code>elif macz is None: tkMessageBox.showerror("Info", "Incorrect Mac Address!")</code>	Kondisi jika tidak Mac Address
28	<code>else: tkMessageBox.showerror("Info", "Incorrect IP and Mac Address!")</code>	Kondisi jika tidak ada IP Address dan Mac Address

Tabel 4.2 menjelaskan bahwa *source code* yang ada yaitu *source code* yang ditampilkan merupakan *source code* yang mewakili keseluruhan *source code* yang dibuat.

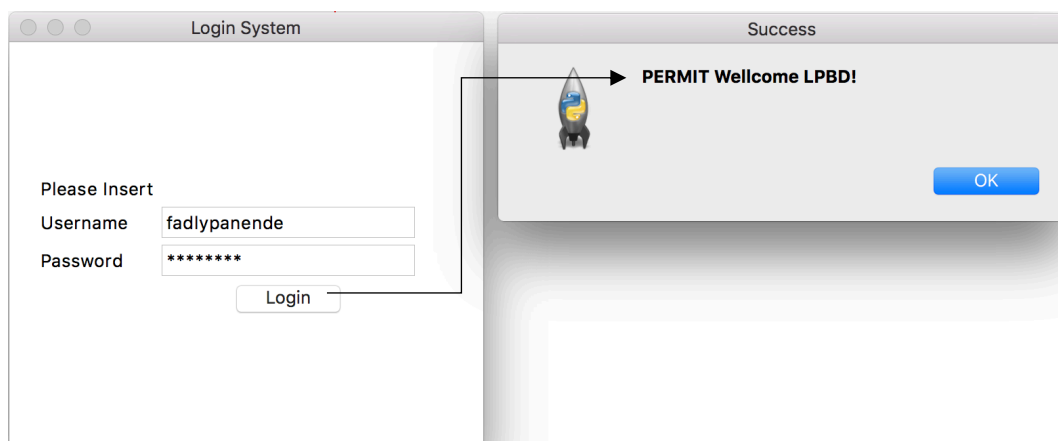
4.5 Implementasi

Sub bab ini menjelaskan tentang implementasi sistem yang dilakukan yakni dengan membuat rancangan *attribute based access control* (ABAC) dengan struktur XACML pada Lemari Penyimpanan Bukti Digital (LPBD). Akses kontrol ini dibuat menggunakan struktur XACML serta bahasa pemrograman *Python* versi 2.7 sebagai *complier*. Penggunaan struktur XACML sangat mengukung untuk memenuhi semua kebutuhan yang digunakan saat merancang akses kontrol *policy* seperti *attribute based access control* (ABAC) (Abd El-Aziz & Kannan, 2013) serta penggunaan bahasa pemrograman *Python* dikarenakan bahasa pemrograman ini dianggap paling cocok digunakan untuk membaca struktur XACML yang dapat diaplikasikan ke dalam sistem operasi yang pada umumnya sering digunakan saat ini, seperti: Microsoft, MacOS dan Linux. Selain itu, penulisan bahasa pemrograman *Python* dinilai lebih sederhana dan ringkas dibanding bahasa pemrograman lain. Gambar 4.40 adalah halaman antar muka *login system*.



Gambar 4.40 Halaman Antar Muka *Login Sytem*

Gambar 4.40 Menjelaskan bahwa halaman *login* yang ditampilkan merupakan halaman awal ketika dilakukannya akses sistem, yang mengharuskan *user* memasukan *username* dan *password* yang dimiliki. Gambar 4.41 merupakan halaman *login success*.



Gambar 4.41 Halaman *Login Success*

Gambar 4.41 Menjelaskan bahwa ketika *username* dan *password* yang dimasukan telah benar dan sesuai dengan kebijakan-kebijakan yang diberikan pada *user* maka proses *login* dinyatakan berhasil. Sebagaimana yang terlihat pada halaman info yaitu “*PERMIT Wellcome LPBD!*”

4.5.1 Implementasi ABAC Pada Sistem LPBD

Sub bab ini akan menjelaskan tentang bagaimana contoh penerapan ABAC pada Aplikasi LPBD yang berkaitan dengan penerapan prosedur dan pemberian hak akses serta *source*

code yang digunakan saat program ABAC dan program LPBD diintegrasikan menjadi satu kesatuan. Sebagaimana yang terlihat pada tabel 4.3 Berikut.

Tabel 4.3 Implementasi Aplikasi LPBD

No	Prosedur	Right	Source Code
1	Upload Digital Evidence	First Responder	<pre>for rooty in sub_target3.getchildren(): ifrooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Upload Digital Evidence']") is not None: reso_fr.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])</pre>
2	Create Cabinet	First Responder	<pre>elifrooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Create Cabinet']") is not None: reso_fr.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])</pre>
3	Download Digital Evidence	Investigator	<pre>for roott in sub_target4.getchildren(): forrootyinsub_target3.getchildren(): ifrooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Download Digital Evidence']") is not None: reso_inv.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])</pre>
4	Complete The Data Coc	Investigator	<pre>for roott in sub_target4.getchildren(): elifrooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Complete The Data Coc']") is not None: reso_inv.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])</pre>
5	Delete Digital Evidence	Officer	<pre>for rooty in sub_target3.getchildren(): ifrooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Delete Digital Evidence']") is not None: reso_off.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])</pre>
6	Change Password User	Officer	<pre>for rooty in sub_target3.getchildren(): Elifrooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Change Password User']") is not None: reso_off.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])</pre>
7	Download Form Coc	Officer Lawyer	<pre>for rooty in sub_target3.getchildren(): elifrooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Download Form Coc']") is not</pre>

Tabel 4.3 Implementasi Aplikasi LPBD (Lanjutan)

No	Prosedur	Right	Source Code
			<pre>None: reso_off.append(rooty.find("./{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])</pre>

Tabel 4.3 Menjelaskan tentang bagaimana contoh penerapan prosedur yang ada pada sistem LPBD yang dispsifikasikan dengan hak akses yang diberikan terhadap *user* sekaligus dengan *source code* yang digunakan pada LPBD dan dilengkapi dengan XACML *policy* (*source code bold*) yang dibuat pada ABAC, hal ini dijelaskan karena untuk dapat dengan mudah dimengerti ketika ABAC yang dirancang ini ingin diintegrasikan pada sistem LPBD yang sebenarnya.

4.5.2 Spesifikasi Komputer yang Digunakan

Pembuatan dan pengujian *attribute based access control* (ABAC) pada LPBD menggunakan laptop dengan merk *Apple*, Tabel 4.4 merupakan spesifikasi laptop yang digunakan:

Tabel 4.4 Spesifikasi Laptop yang Digunakan

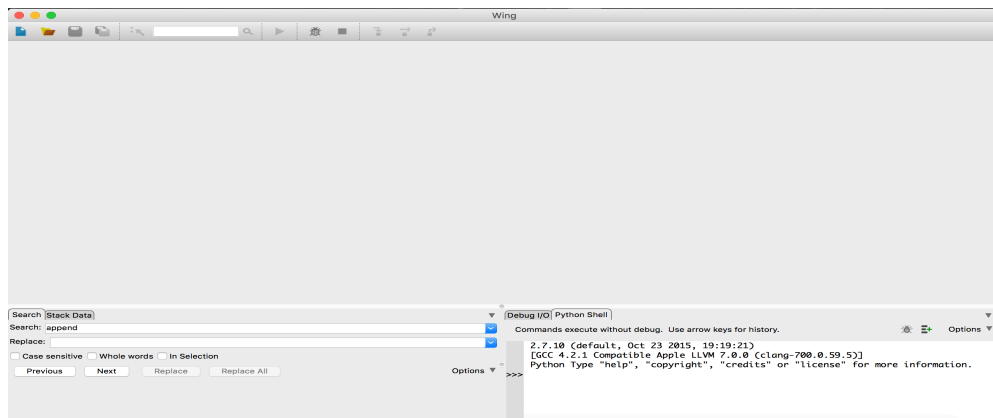
No	Komponen	Deskripsi
1.	Nomor Serial Laptop	C02S7528FVH5
2.	Ukuran Layar	13.3 inch Retina Display
3.	Grafis	Intel Iris Graphics 6100 1536 MB
4.	Resolusi	2560 x 1600
5.	Prosesor	2.7 Dual-Core Intel Core i5 (Turbo Boost 3.1 GHz)
6.	Kapasitas RAM	8 GB 1867 MHz DDR3
7.	Port	MagSafe 2 Power Port, 2 Thunderbolt 2 Ports, 2 USB 3 Ports, HDMI Port, 3.5 mm Headphone Jack, SDXC Card Slot, Apple Thunderbolt to FireWire Adapter, Apple Thunderbolt to Gigabit Ethernet Adapter
8.	Koneksi	Wi-Fi 802.11ac IEEE 802.11a/b/g/n, Bluetooth 4.0 Wireless Technology
9.	Optical Drive	DVD Writer
10.	Berat	1,58 Kg

Sistem operasi yang digunakan untuk membuat rancangan *attribute based access control* (ABAC) pada LPBD adalah MacOS X El Capitan Versi 10.11.6. Sistem operasi ini termasuk bagian dari Macintosh yang merupakan sistem operasi buatan Apple dan dirilis pada tanggal 30 September 2015. Macintosh merupakan salah satu sistem operasi yang tahan terhadap

serangan virus dan memiliki *graphical user interface* (GUI) yang menarik, sehingga dapat dengan mudah digunakan. Pengguna juga dapat melakukan *upgrade* macintosh tanpa melakukan pembayaran.

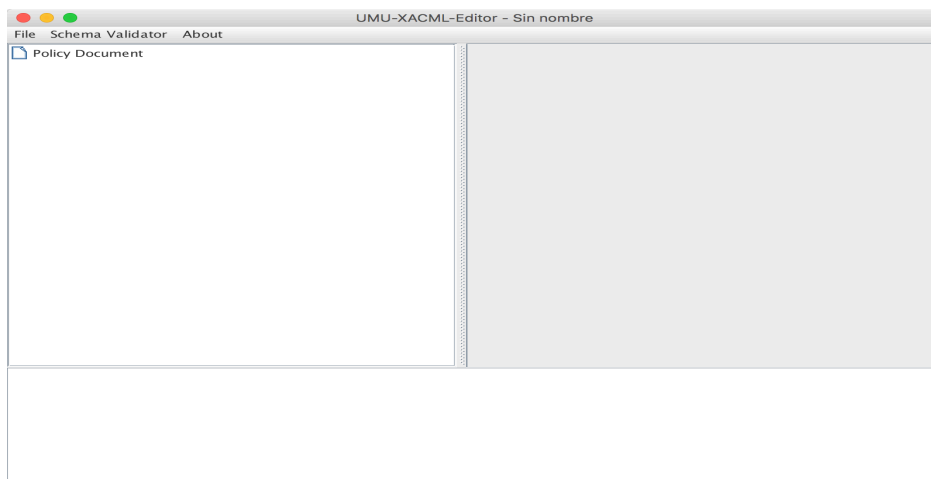
4.5.3 Jenis *Complier*

Complier merupakan aplikasi yang digunakan untuk menerjemahkan bahasa pemrograman (*source code*) kedalam bahasa objek (*object code*). *Compiler* yang digunakan untuk membuat rancangan *attribute access control* (ABAC) pada LPBD adalah Wing 101 Versi 6.0.2-1. Aplikasi ini dikhususkan untuk membuat aplikasi dengan menggunakan bahasa pemrograman Python. Gambar 4.42 menunjukkan halaman awal Wing 101.



Gambar 4.42 Halaman Awal Wing 101

Gambar 4.43 Berikut merupakan halaman utama UMU-XACML-Editor Versi 1.3.2 yang digunakan untuk membuat struktur XACML *policy*.



Gambar 4.43 Halaman Utama UMU XACML Editor- Sin Nombore

4.6 Simulasi dan Skenario Kasus

Tahapan simulasi dan skenario kasus ini dilakukan untuk dilakukannya pengujian akses kontrol yang buat, yaitu bagaimana menyesuaikan antara kebutuhan akses kontrol dan kebutuhan sistem LPBD. Ada 4 *user* yang dideskripsikan sebagai aktor yaitu *first responder*, *Investigator*, *officer* dan *lawyer*. Yang dimana masing-masing dari *user* tersebut mempunyai kewenangan tersendiri terhadap sistem LPBD. Tabel 4.5 menjelaskan tentang simulasi kasus yang pertama.

Tabel 4.5 Simulasi Kasus 1

User	Subject	Resource	Actions	Environment	Output
First responder	√	√	√	√	Permit
Investigator	√	√	√	√	Permit
Officer	√	√	√	√	Permit
Lawyer	√	√	√	√	Permit

Tabel 4.5 Simulasi kasus 1 menjelaskan bahwa ketika *user* jabatan *first responder*, *investigator*, *officer* maupun *lawyer* melakukan *request* pada LPBD dapat memenuhi semua kebijakan yang diterapkan pada akses kontrol melalui komponen elemen *subject*, *resource*, *action* dan *environment* maka *output* yang dihasilkan adalah *permit*. Selanjutnya simulasi kasus yang kedua. Tabel 4.6 menjelaskan tentang simulasi kasus yang kedua.

Tabel 4.6 Simulasi Kasus 2

User	Subject	Resource	Action	Environment	Output
First Responder	√	-	√	-	Deny
Investigator	√	√	-	-	Deny
Officer	√	-	√	√	Deny
Layer	√	√	√	-	Deny

Tabel 4.6 Simulasi kasus 2 menjelaskan bahwa ketika *user* *first responder*, *investigator*, *officer*, *lawyer* melakukan *request* pada LPBD dan tidak dapat memenuhi satu atau lebih persyaratan kebijakan yang telah diberikan melalui komponen *elemen subject*, *resource*, *action*, dan *environment* maka *output* yang dihasilkan adalah *deny*.

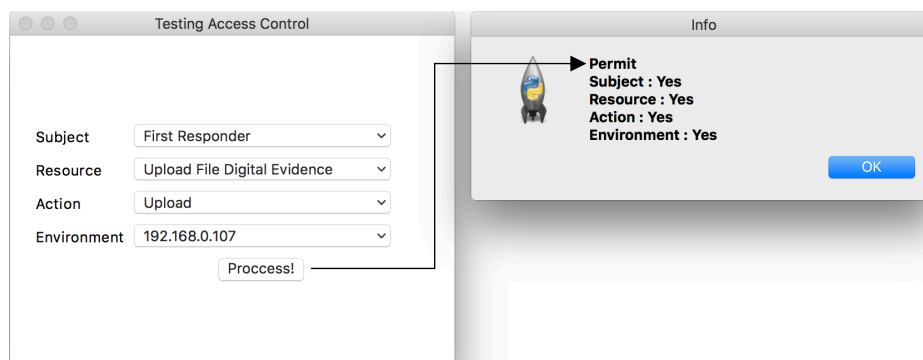
Dari 2 simulasi kasus yang dijelaskan diatas, bahwa setiap *user* diwajibkan memenuhi aturan kebijakan yang diterapkan pada akses kontrol. Kebijakan-kebijakan yang menjadi atribut tersebut merupakan komponen-komponen utama yang ada pada sistem LPBD.

4.7 Pengujian Akses Kontrol

Pengujian akses kontrol pada LPBD dilakukan menggunakan *tools* khusus untuk menguji kinerja akses kontrol LPBD, pada dasarnya hanya ada dua kemungkinan *decision* ketika subjek melakukan permintaan akses terhadap objek yaitu kondisi *permit* dan *deny* (Hu et al. 2014). Rangkaian pengujian akses kontrol LPBD ini akan dikategorikan baik ketika kondisi yang dihasilkan adalah *permit*, begitupun sebaliknya jika kondisi yang dihasilkan adalah *deny* maka akan dikategorikan tidak baik. Adapun rangkaian pengujian akses kontrol yang dilakukan yaitu menggunakan 4 sample data kondisi *permit* dan 4 sample data kondisi *deny* yang diuji coba menggunakan 4 *user* yaitu *first responder*, *investigator*, *officer*, *lawyer*. Pengujian yang dilakukan berdasar pada penjabaran yang ada pada simulasi dan skenario. Pengujian ini juga memiliki keterbatasan pada saat melakukan perubahan terhadap atribut *policy* yang berkaitan dengan perubahan kebijakan akses, pengujian ini juga hanya dapat dilakukan menggunakan desain awal *policy*, jika sewaktu-waktu kebijakan yang ada pada *policy* akan dirubah, maka proses yang akan dilakukan yaitu mengubah struktur XACML *policy* sebagai proses awal melalui UMU XACML editor, kemudian disimpan dalam bentuk *file.XML* dan cocokan kembali dengan *source code* yang sudah disiapkan pada *tools* pengujian akses kontrol ini dalam bentuk *file.XHTML*.

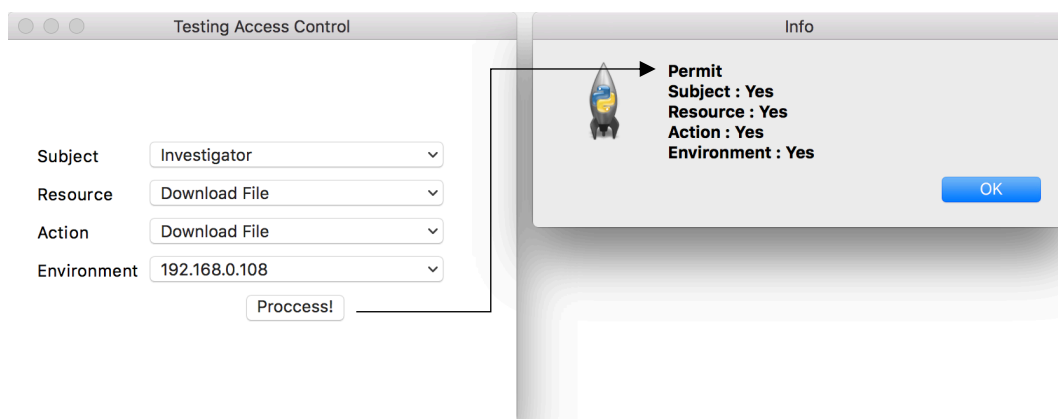
4.7.1 Pengujian Kondisi *Permit*

Pengujian sample kondisi *permit* diawali dengan menguji *user fist responder*. Sebagaimana yang terlihat pada gambar 4.44.



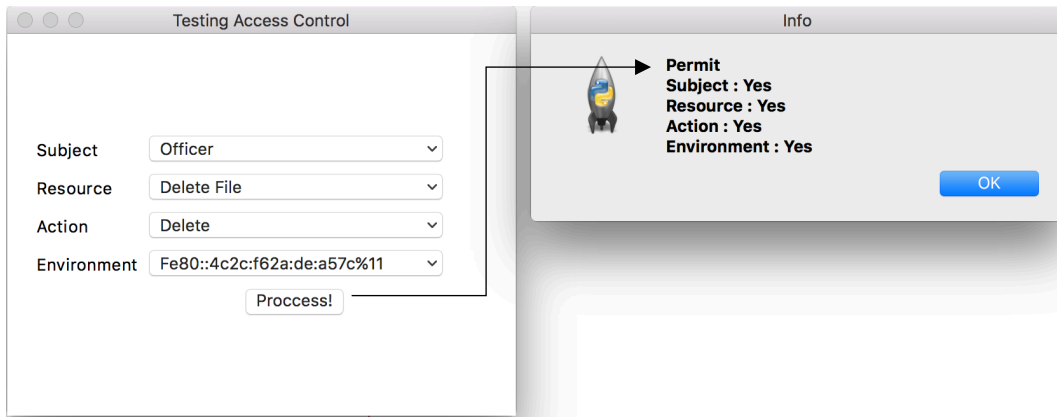
Gambar 4.44 Sample Hasil Pengujian *Permit* 1

Gambar 4.44 menjelaskan bahwa pada pengujian kondisi *permit* yang pertama ketika melakukan “klik” tombol *process* maka kondisi yang dihasilkan yaitu *permit* dikarenakan semua atribut yang dimasukkan benar seperti yang terlihat pada halaman info *permit subject: yes resource: yes action: yes* dan *environment: yes* atribut yang dimasukkan diatas merupakan atribut yang mewakili keseluruhan atribut yang ada pada *rules*. atribut yang telah disematkan pada *user first responder*, attribute yang dimasukkan yaitu *subject: first responder, resource: upload file digital evidence, actions: upload*, dan *environment: ip address: 192.168.0.107*. Selanjutnya melakukan pengujian sample kondisi *permit* yang kedua dengan menguji *user investigator*. Sebagaimana yang terlihat pada gambar 4.45.



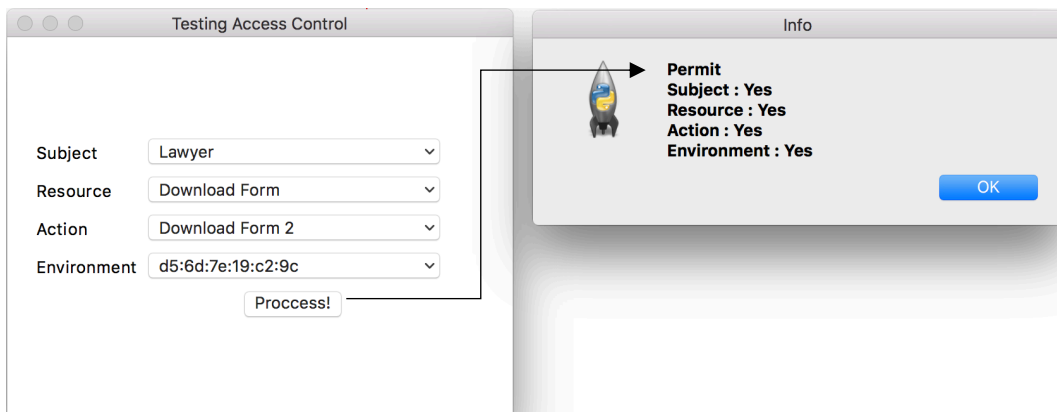
Gambar 4.45 Sample Hasil Pengujian *permit* 2

Gambar 4.45 menjelaskan bahwa pada pengujian kondisi *permit* yang kedua ketika melakukan “klik” tombol *process* maka kondisi yang dihasilkan yaitu *permit* dikarenakan semua atribut yang dimasukkan benar seperti yang terlihat pada halaman info *permit subject: yes resource: yes action: yes* dan *environment: yes* atribut yang dimasukkan diatas merupakan atribut yang mewakili keseluruhan atribut yang ada pada *rules*. atribut yang telah disematkan pada *user investigator*, atribut yang dimasukkan yaitu *subject: investigator, resource: download, actions: download file*, dan *environment: ip address: 192.168.0.108*. Setelah melakukan pengujian pada *user investigator*, dilanjutkan dengan menguji sample kondisi *permit* ketiga menggunakan *user* yang ketiga yaitu *user officer*. Sebagaimana yang terlihat pada gambar 4.46.



Gambar 4.46 Sample Hasil Pengujian Permit 3

Gambar 4.46 menjelaskan bahwa pada pengujian kondisi *permit* yang ketiga ketika melakukan “klik” tombol *process* maka kondisi yang dihasilkan yaitu *permit* dikarenakan semua atribut yang dimasukkan benar seperti yang terlihat pada halaman info *permit* *subject: yes resource: yes action: yes* dan *environment: yes* atribut yang dimasukkan diatas merupakan atribut yang mewakili keseluruhan atribut yang ada pada *rules*. atribut yang telah disematkan pada *officer*, attribute yang dimasukkan yaitu *subject: officer, resource: delete file, actions: delete* dan *environment: mac address: Fe80::4c2c:f62a:de:a57c%11*. Pengujian sample kondisi *permit* yang terakhir yaitu menguji *user lawyer*, sebagaimana yang terlihat pada gambar 4.47.



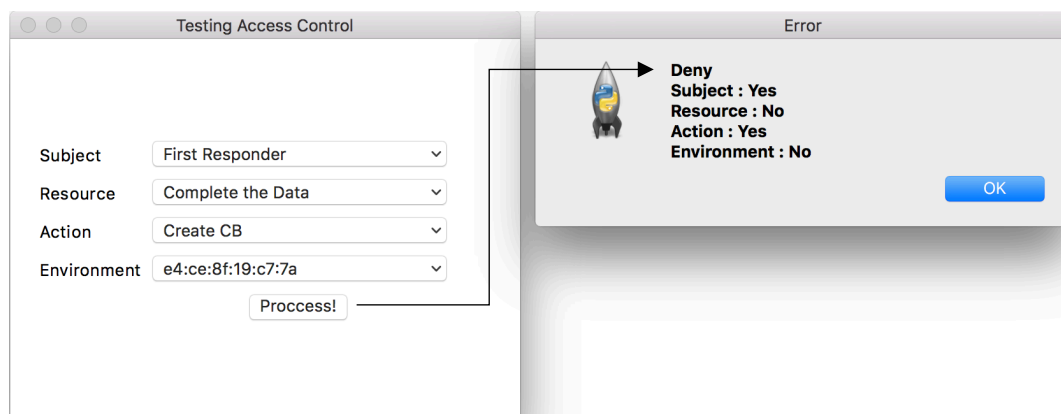
Gambar 4.47 Sample Hasil Kondisi Permit 4

Gambar 4.47 menjelaskan bahwa pada pengujian kondisi *permit* yang ke empat ketika melakukan “klik” tombol *process* maka kondisi yang dihasilkan yaitu *permit* dikarenakan semua atribut yang dimasukkan benar seperti yang terlihat pada halaman info *permit* *subject: yes resource: yes action: yes* dan *environment: yes* atribut yang dimasukkan diatas merupakan atribut yang mewakili keseluruhan atribut yang ada pada *rules*. atribut yang telah disematkan

pada *lawyer*, atribut yang dimasukan yaitu *subject: lawyer, resource: download form, , actions: download form2*, dan *environment: mac address: d5:6d:7e:19:c2:9c*.

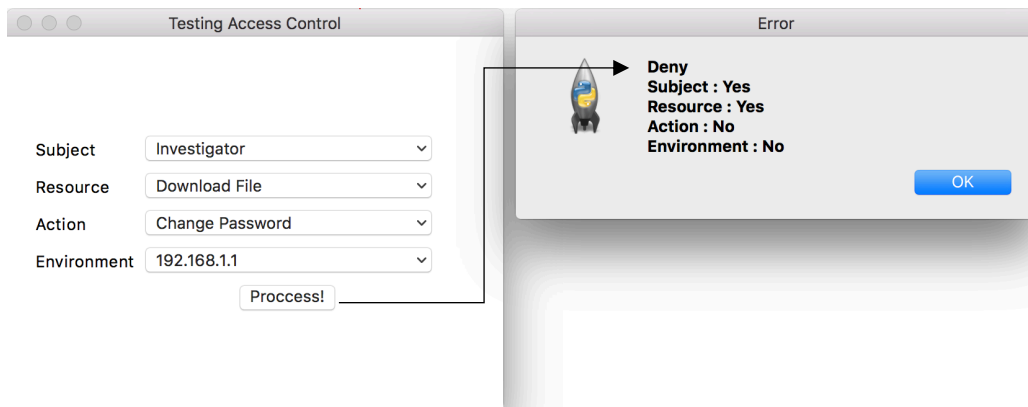
4.7.2 Pengujian Kondisi *Deny*

Sampel pengujian kondisi *deny* yang pertama yang dilakukan menggunakan *user first responder*, ketika melakukan “klik” tombol *process* kondisi yang dihasilkan adalah *deny* sebagaimana yang terlihat pada halaman info bahwa *subject: yes, resource: no, actions yes* dan *environment: no* terdapat 2 kesalahan yaitu pertama terdapat pada inputan *resource* yang diisi dengan *complete data* dan kesalahan kedua ditemukan pada inputan *environment* yang diisi dengan *e4:ce:8f:19:c7:7a* hal ini disebabkan bahwa atribut *resource* dan *environment* yang dimasukan bukan merupakan atribut dari *investigator*. Gambar 4.48 berikut merupakan sample hasil pengujian kondisi *deny* yang pertama.



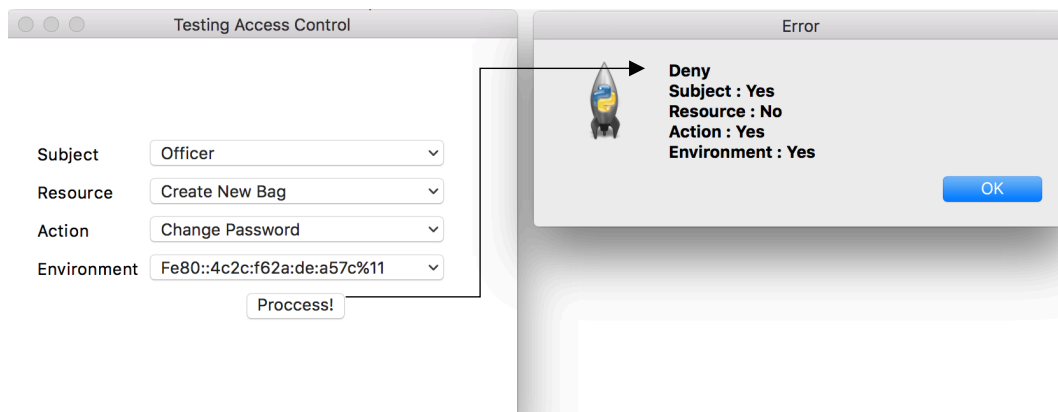
Gambar 4.48 Sample Pengujian *Deny* 1

Sample pengujian kondisi *deny* kedua yang dilakukan menggunakan *user investigator*, ketika melakukan “klik” pada tombol *process* maka kondisi yang akan ditemukan adalah *deny* sebagaimana yang terlihat pada halaman info bahwa *subject:yes, resource:yes, actions:no, environment:no*. terdapat 2 kesalahan pada saat memasukan atribut, kesalahan yang pertama yaitu *action* yang diisi dengan *change password*, dan kesalahan yang kedua terdapat pada isian *environment* yang diisi dengan *192.168.1.1* hal ini terjadi karena atribut *action* dan *environment* yang dimasukan bukan merupakan atribut yang disematkan pada *subject investigator*. Gambar 4.49 merupakan tampilan kondisi *deny* yang kedua.



Gambar 4.49 Sample Hasil Pengujian *Deny* 2

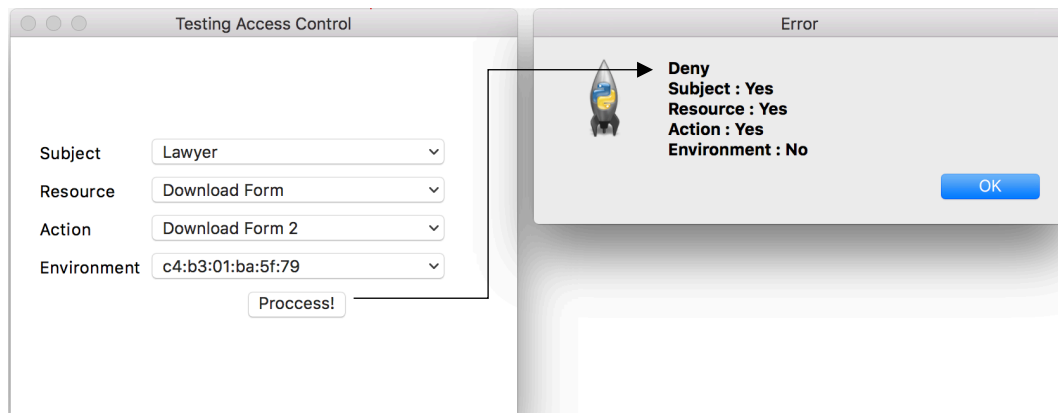
Pengujian sample kondisi *deny* yang ketiga dilakukan menggunakan *user officer*, ketika “klik” tombol *process* maka hasil yang didapatkan adalah *deny* sebagaimana yang terlihat pada halaman info bahwa *subject: yes, resource: no, action: yes, environment: yes* terdapat 1 kesalahan pada inputan ini yaitu inputan pada atribut *resource* yang diisi dengan *create new bag*. Kondisi *deny* ini terjadi dikarenakan atribut *resource* yang dimasukkan bukan merupakan atribut *resource* yang disematkan pada *officer*. Gambar 4.50 adalah tampilan kondisi *deny* yang tiga.



Gambar 4.50 Sample Hasil Pengujian *Deny* 3

Sample pengujian kondisi *deny* yang keempat dilakukan menggunakan *user lawyer*, ketika “klik” tombol *process* ditemukan kondisi *deny*, sebagaimana yang terlihat pada halaman info yaitu *subject: yes, resource: yes, actions: yes, environment: no*. Terdapat 1 kesalahan pada masukan atribut yaitu pada atribut *environment* yang diisi dengan *c4:b3:01:ba:5f:79*. Kondisi *deny* ini terjadi disebabkan atribut *resource* yang dimasukkan bukan merupakan

atribut *resource* yang disematkan pada *lawyer*. Berikut tampilan kondisi *deny* yang keempat, terlihat pada gambar 4.51.



Gambar 4.51 Sample Hasil Pengujian *Deny* 4

4.8 Hasil dan Analisis

Sub bab ini menjelaskan mengenai hasil yang didapatkan setelah melakukan serangkaian pengujian akses kontrol dan analisis merupakan tahapan yang dilakukan setelah melakukan tahapan implementasi.

4.8.1 Hasil

Berdasarkan hasil pengujian akses kontrol yang telah dijabarkan sebelumnya bahwa akses kontrol yang telah diuji menggunakan *tools* pengujian telah berjalan dengan baik sebagaimana mestinya. Uji fungsional menggunakan sample data uji yang dilakukan melalui rangkaian skenario dan simulasi serta pengujian. hasil yang di dapatkan terlihat pada tabel hasil pengujian dibawah ini. Tabel 4.7 menjelaskan hasil pengujian *permit*.

Tabel 4.7 Hasil Pengujian *Permit*

Subject	Resource	Actions	Environment	Output
First Responder	Upload File Digital Evidence	Upload	Ip Address: 192.168.0.107	Permit
Investigator	Download File Digital Evidence	Download File	Ip Address: 192.168.0.108	Permit
Officer	Delete File	Delete	Mac Address: Fe80::4c2c:f62a:de:a57c%11	Permit

Tabel 4.7 Hasil Pengujian *Permit* (Lanjutan)

Subject	Resource	Actions	Environment	Output
Lawyer	Download Form Coc	Download Form2	Mac Address: d5:6d:7e:19:c2:9c	Permit

Tabel 4.7 Menjelaskan bahwa jika komponen atribut yang disematkan pada *user* dinyatakan benar maka hasil yang didapatkan yaitu *permit*.

Tabel 4.8 berikut menjelaskan bahwa kondisi *deny* disebabkan tidak sesuainya antara atribut yang dimasukkan dan atribut yang sebenarnya telah disematkan, seperti kesalahan pada inputan atribut yang diberikan pada *first responder* yaitu *resource: complete the data coc* yang pada kondisi sebenarnya resource tersebut diisi dengan *create cabinet*, pada *investigator* kesalahan pada *action* dan *environment* yang diisi dengan *change password* dan *ip address: 192.168.1.1* yang pada kondisi sebenarnya yang harus dimasukkan adalah *download file* dan *192.168.0.108*. *Officer* kesalahan pada inputan *actions* yang diisi dengan *create new bag* yang pada kondisi sebenarnya harus diisi dengan *changer password user*. *Lawyer* kesalahan terdapat pada inputan *envioronment* yang diisi dengan *c4:b3:01:ba:5f:79* yang pada kondisi sebenarnya harus diisi dengan *d5:6d:7e:19:c2:9c*. Kesalahan inputan diberi tanda *highlight* warna kuning.

Tabel 4.8 Hasil Pengujian *Deny*

Subject	Resource	Actions	Environment	Output
First Responder	Complete The Data Coc	Create CB	Mac Address: e4:ce:8f:19:c7:7a	Deny
Investigator	Download File Digital Evidence	Change Password	Ip Address: 192.168.1.1	Deny
Officer	Create New Bag	Change Password	Mac Address: Fe80::4c2c:f62a:de:a57c%11	Deny
Lawyer	Download Form Coc	Download Form2	Mac Address: c4:b3:01:ba:5f:79	Deny

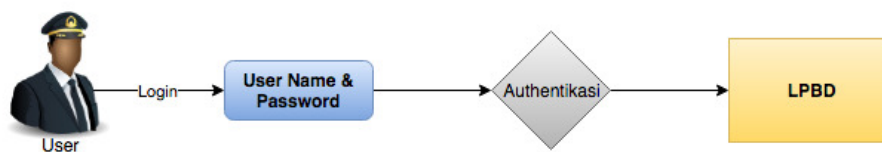
4.8.2 Analisis

Tahapan analisis ini menjelaskan tentang solusi-solusi dari masalah yang ada berdasarkan data yang didapatkan. Terdapat 3 aspek utama yang menjadi fokus penelitian ini yaitu

analisis perbandingan akses kontrol sebelumnya dengan akses kontrol yang baru, *policy statement*, dan *XACML policy*.

1. Analisis Perbandingan Akses Kontrol

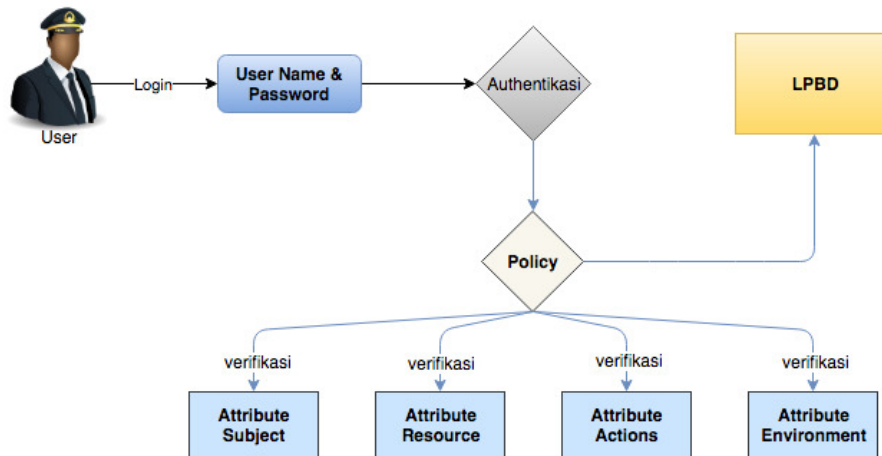
Berdasarkan permasalahan yang terdapat pada latar belakang penelitian ini bahwa terdapat permasalahan pada akses kontrol LPBD sebelumnya, yang dibuat hanya dengan mekanisme autentikasi dan authorisasi *user* saja, tidak adanya parameter lain yang mendukung proses autentifikasi dan authorisasi yang lebih kompleks. LPBD seharusnya dibuat tidak hanya berdasar pada permasalahan-permasalahan tentang manajemen bukti digital saja, akan tetapi komponen-komponen penting lainnya dalam lemari penyimpanan bukti digital itu sendiri yaitu pengaturan pada aksesnya. Hal ini karena sistem LPBD menyimpan bukti digital yang tidak semua orang dapat mengaksesnya. Gambar 4.52 menunjukkan akses kontrol pada sistem LPBD sebelum dilakukan perubahan akses kontrol.



Gambar 4.52 Akses Kontrol LPBD Sebelumnya

Model *attribute based access control* (ABAC) yang usulkan pada LPBD saat ini, merupakan sebuah solusi model akses kontrol yang lebih tepat untuk model sistem seperti LPBD, dikarenakan ABAC merupakan model akses kontrol yang lebih fleksibel dalam penerapan atribut terhadap *user*, *object*, dan kondisi lingkungan (Hu, Kuhn, & Ferraiolo, 2015). Hal ini telah sesuai dengan apa yang dikerjakan saat ini, bahwa model *attribute based access control* (ABAC) yang dirancang khusus untuk LPBD telah menerapkan aturan *policy* berupa atribut *subject*, *resource*, *action* dan *environment*. Hal ini karena sebuah *request* akses tidak hanya memenuhi autentifikasi *user* saja, akan tetapi wajib memenuhi *rule policy* yang telah diberikan sebagai authorisasi terhadap *object* yang ada. Selain itu terdapat beberapa aspek lain dalam perizinan akses yang dapat dijadikan parameter dan solusi, bahwa ABAC juga dapat memilah dimana proses autentikasinya terfokus pada verifikasi terhadap klaim identitas *user*, dan authorisasinya terfokus pada pemberian hak akses terhadap *resource*, sementara akses kontrol fokusnya pada proteksi keamanan dari *resource* tertentu, yaitu

sebuah mekanisme untuk memastikan bahwa *user* tidak melakukan tindakan tertentu yang tidak sesuai dengan *policy* umum keamanan yang diterapkan. Dengan adanya rancangan ABAC pada LPBD ini juga dapat meningkatkan tingkat keamanan sistem LPBD yang berisi bukti digital yang harus tetap terjaga keasliannya. Gambar 4.53 merupakan tampilan model akses kontrol yang baru.



Gambar 4.53 Akses Kontrol yang Baru

Tabel 4.9 menjelaskan tentang apa saja komponen-komponen yang dapat dibandingkan antara akses kontrol sebelumnya dan model akses kontrol yang diusulkan.

Tabel 4.9 Perbandingan Akses Kontrol

Komponen	Access Control		Keterangan
	Lama	Baru	
<i>Username</i>	√	√	
<i>Password</i>	√	√	
Authetifikasi	√	√	
Authorisasi	√	√	
<i>Rule Policy</i>		√	Aturan Kebijakan Terhadap User
<i>Attribute Subject</i>		√	Berisi kebijakan berupa identitas <i>user</i>
<i>Attribute Resource</i>		√	Berisi Identitas Resource
<i>Attribute Actions</i>		√	Actions yang pada resource
<i>Attribute Environment</i>		√	Berisi identitas device dan waktu pembagian waktu akses

2. Analisis Policy Statement

Berdasarkan penjelasan tentang *policy statement* yang telah jabarkan sebelumnya bahwa usulan *policy statement* pada akses kontrol LPBD menjadi sangat penting dalam merancang sebuah rancangan ABAC hal ini, sebagaimana yang disebutkan oleh (Taylor et al. 2007) bahwa sebuah *policy statement* yang secara jelas menspesifikasikan apa yang boleh dan apa yang tidak boleh di akses dalam lingkup keamanan. Untuk itu *policy statement* yang diusulkan pada *access control* LPBD yaitu menyesuaikan antara kebutuhan akses kontrol dan kebutuhan yang ada pada LPBD itu sendiri, pengujian *policy statement* dikatakan berfungsi dengan baik ketika semua komponen kebutuhan akses kontrol dan LPBD telah terpenuhi. Kebutuhan-kebutuhan tersebut telah diimplementasikan dan dilakukan pengujian melalui rangkaian simulasi kasus dan pengujian akses kontrol. Bahwa *policy statement* digunakan telah diuji dan dinyatakan sesuai dengan apa yang dibutuhkan oleh sistem LPBD sebagaimana yang terlihat pada tabel 4.10.

Tabel 4.10 Usulan Nilai Atribut

Subject	Resource	Actions	Environment	Output
First Responder	Upload Digital Evidence	Upload	Ip Address: 192.168.0.107 Mac Address: c4:b3:01:ba:5f:79 Time Access: 24	Ok
	Create New Cabinet	Create		Ok
	Create New Rack	Create		Ok
	Create New Bag	Create		Ok
	Input Data Coc	Input		Ok
Investigator	Download Digital Evidence	Download	Ip Address: 192.168.0.108 Mac Address: e4:ce:8f:19:c7:7a Time Access: 24	Ok
	Complete The Data Coc	Complete The Data		Ok
Officer	Delete Digital Evidence	Delete	Ip Address: 192.168.1.1 MacAddress: Fe80::4c2c:f62a:d e:a57c%11 Time Access: 24	Ok
	Change Password User	Change Password		Ok
	Validate Digital Evidence	Validate		Ok
	Download Form Coc	Download		Ok
	Validate Case Status	Validate		Ok
	Change Code Signature	Change Code		Ok
	Validate Data Coc	Validate		Ok

Tabel 4.10 Usulan Nilai Atribut (lanjutan)

Subject	Resource	Actions	Environment	Output
Lawyer	Download Form Coc	Download	Ip Address: 192.168.0.106 Mac Address: d5:6d:7e:19:c2:9c TimeAccess: 09.00-15.00	Ok

Tabel 4.10 menjelaskan bahwa semua *policy statement* yang di usulkan sebelumnya telah berjalan dan berfungsi dengan baik sebagaimana mestinya yang diharapkan bahwa *policy statement* yang di usulkan dapat digunakan sebagai nilai dari atribut yang disematkan.

3. Analisis XACML Policy

Berdasarkan penjelasan perancangan struktur XACML *policy* yang telah dijabarkan sebelumnya bahwa salah satu fleksibilitas terhadap penggunaan ABAC sebagai model akses kontrol adalah adanya standard bahasa XML untuk mendukung desain akses kontrol *policy* dan penggunaan ABAC sebagai model akses kontrol, yaitu XACML (Abd El-Aziz & Kannan, 2013). XACML yang telah diterapkan dengan melihat hasil struktur XACML yang telah dibuat menggunakan UMMU XACML Editor V.1.3.2, hasil yang didapatkan yaitu bahwa XACML yang dibuat telah berhasil dikeluarkan dalam format.xml. Hasil uji fungsional XACML yang dibuat telah sesuai dengan kebutuhan akses kontrol yang yang di terapkan pada LPBD, disebabkan struktur XACML yang dibuat telah dapat diimplementasikan menjadi sebuah rangkaian pengaturan akses berupa sebuah halaman *login* berdasarkan rangkaian uji coba fungsional. Sebagaimana yang terlihat pada tabel 4.11.

Tabel 4.11 Analisis XACML Policy LPBD

Elemen	Isian	Berfungsi	
		Ya	Tidak
Xmlns	Policy_schema	√	
PolicyId	Access_control_policy_LPB D	√	
Rule combining algorithm	First applicable	√	
Rules	RuleId & Effect	√	
subjectMatch	MatchId	√	
AttributeValue	Data type & value	√	

Tabel 4.11 Analisis XACML *Policy* LPBD (Lanjutan)

Elemen	Isian	Berfungsi	
		Ya	Tidak
SubjectAttributeDesignator	AttributeID, data type, issuer	√	
ResourceMatch	MatchId	√	
Attribute Value	Data type & value	√	
ResourceAttributeDesignator	AttributeId, data type, issuer	√	
ActionMatch	MatchId	√	
Attribute Value	Data type & value	√	
ActionsAttributeDesignator	AttributeId, data type, issuer	√	
EnvironmentMatch	MatchId	√	
AttributeValue	Data type & value	√	
EnvironmentAttributeDesignstor	AttributeId, data type, issuer	√	

Tabel 4.10 menjelaskan bahwa XACML *policy* yang dibangun menggunakan 1 *policy* dan 1 *rule*, untuk penggunaan aturan *first applicable* pada *rule combining applicable* dikarenakan untuk dapat mengatasi terjadinya konflik antar elemen pada 1 himpunan *policy* dan *rule* yang sama, penggunaan 1 *rule* pada 1 *policy* bertujuan agar dapat mempermudah jika sewaktu-waktu dilakukan penambahan jumlah *user* pada 1 jabatan yang sama serta dilengkapi dengan 4 *attribute predefined* yaitu : *subject, resource, action* dan *environment* yang berguna untuk menentukan *attribute* yang digunakan pada akses kontrol LPBD.

BAB 5

Kesimpulan

5.1 Kesimpulan

Berdasarkan penjelasan rancangan model *attribute based access control* (ABAC) pada lemari penyimpanan bukti digital (LPBD) yang telah dijabarkan sebelumnya, maka dapat disimpulkan bahwa :

1. Perancangan ABAC pada LPBD ini diawali dengan melakukan perancangan model ABAC, dilanjutkan dengan membuat konsep XACML *policy* untuk dapat menyesuaikan antara kebutuhan ABAC dan kebutuhan sistem LPBD, serta diimplementasikan dalam bentuk model halaman *login* pada LPBD. Pendekatan menggunakan metode ABAC pada LPBD ini juga dapat menjadi solusi atas permasalahan akses kontrol LPBD yang dibuat sebelumnya.
2. Berdasarkan hasil pengujian ABAC dengan sampel data uji melalui rangkaian skenario, simulasi dan pengujian kinerja akses kontrol menggunakan *tools* yang dibuat khusus untuk menguji kinerja ABAC pada LPBD ini, didapatkan hasil bahwa akses kontrol yang dibuat telah berjalan dengan baik dan berfungsi sebagaimana mestinya yang diharapkan. Selain itu pendekatan menggunakan metode ABAC ini juga dapat menjadi solusi dalam meningkatkan tingkat keamanan sistem LPBD khususnya dalam hal identifikasi *user*.

5.2 Saran

Adapun saran bagi peneliti selanjutnya yang berkenan mengembangkan akses kontrol yang telah dibuat ini, perlu memperhatikan beberapa faktor berikut ini yaitu:

1. Akses kontrol ini belum dilengkapi dengan uji coba *schema* rancangan XACML, untuk itu perlu dilakukan penelitian yang berkaitan dengan *schema* struktur XACML yang ada.
2. Selain melakukan pengujian *schema* struktur XACML, perlu juga melakukan validasi terhadap rancangan struktur XACML yang telah dibuat.

Daftar Pustaka

- Younis , A., Kifayat, Kashif,. & Merabti, Madjid,. (2013). An Access Control Model for Cloud Computing, *Journal of Information Security and Applications*, 45-60.
- Kannan, A., Abd El-Aziz, A.A,. (2013). A Comprehensive Presentation to XACML, Third International Conference on Computational Intelligence and Information Technology (CIIT), 155-161.
- Prayudi, Y. (2014). Problema dan Solusi Digital Chain Of Custody. *Seminar Nasional Aplikasi Teknologi Informasi (Senasti)*, 197.
- Widatama, K,. & Prayudi, Y. (2017). Konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML..*Seminar Nasional Informatika dan Aplikasinya (SNIA) ke-3 dengan tema "Digital Evidence and Computer Crime*, 23.
- Yudi, P., Ahmad, A., & Tri, K. P. (2014). Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody. *International Journal of Computer Applications*, 30-36.
- Yudi, P., & Azhari, S. (2015). Digital Chain of Custody: State of the Art. *International Journal of Computer Applications*, 1-9.
- Yudi, P., & Tri, K. P. (2015). Secure and Trusted Environment as a Strategy to Maintain the Integrity and Authenticity of Digital Evidence. *International Journal of Security and Its Applications*, 299-214.
- Dianxiang Xu, Y. Z. (2014). *Specification and Ananalysis of Attribute-Based Access Control Policies: An Overview*. USA.
- Yan zhu, D. H. (2015). *From RBAC to ABAC: Constructing Flexible Data*.
- Khalid Zaman Bijon, R. K. (n.d.). *Constraint Specification in Attribute Based Access Control*.
- Ni dan, S. H. (2012). Attribute Based Access Control (ABAC)-Based Cross-Domain Access Control in Service-Oriented Architecture. *International Conference on Computer Science and Servie System*.
- Mike Burmester, E. M. (2013). T-ABAC: An attribute-based access control model for real-time availability in highly dynamic systems. *Symposium on Computers and Communications (ISCC)*.
- W. Smari, P. C. (2014). An Extended Attribute Based Access Control Model with Trust and Privacy: Application to a Collaboration Crisis Management System. *Future Generation Coputer Systems*.

- Xuang Son HA, I. K. (2016). Rew-XAC: An Approach to Rewriting Request for Elastic ABAC Enforcement with Dynamic Policies. *International Conference on Advanced Computing and Applications (ACOMP)*.
- Khaled Riad, Z. Y. (2015). AR-ABAC: A New Attribute Based Access Control Model Supporting Attribute-Rules for Cloud Computing. *Conference on Collaboration and Internet Computing*.
- Hui Qi, X. L. (2016). Access Control Model Based on Role and Attribute and Its Implementation. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*.
- Robayet Nasim, S. B. (2014). XACML-Based Access Control for Decentralized Online Social Networks. *International Conference on Utility and Cloud Computing*.
- Koch, M. E. (2008). UML modelling of digital forensic process models (DFPMs). *Proceedings of the ISSA Innovative Minds Conference*.
- Marshall, A. M. (2008). Digital Forensics : *Digital Evidence in Criminal Investigation*.
- Morioka, E., & Sharbaf, M. S. (2016). Digital Forensics Research on Cloud Computing : An investigation of Cloud Forensics Solutions. *IEEE Symposium on Technologies for Homeland Security (HST)*, 1–6
- Sandhu, Ravi. 2010. "Security Models : Past , Present and Future." (August):1–28. Stallings, William and Lawrie Brown. 2015. *Computer Security : Principles and Practice*. 3rd Editio. USA: Pearson Education International.
- Priebe, Torsten, Wolfgang Dobmeier, Christian Schläger, and Nora Kamprath. 2007. "Supporting Attribute-Based Access Control in Authorization and Authentication Infrastructures with Ontologies." *Journal of Software* 2(1):27–38.
- Hu, Vincent C. et al. 2014. "Guide to Attribute Based Access Control (ABAC) Definition and Considerations." *NIST Special Publication* 800:162.
- Taylor, Carol, Barbara Endicott-Popovsky, Deborah A. Frincke, and Dummy. 2007. "Specifying Digital Forensics: A Forensics Policy Approach." *Digital Investigation* 4:101–4.
- Henim, Silvana Rasio. 2016. "Membangkitkan XACML Request Menggunakan Framework X-CREATE."
- Lorch, Markus, Seth Proctor, Rebekah Lepro, Dennis Kafura, and Sumit Shah. 2003. "First Experiences Using XACML for Access Control in Distributed Systems." *Proceedings*

of the 2003 ACM Workshop on XML Security (C):25–37.

Nergaard, Henrik and Nils Ulltveit-moe. 2015. “A Scratch-Based Graphical Policy Editor for XACML.” *Proceedings of the 1st International Conference on Information Systems Security and Privacy* (March):182–90. Retrieved (<http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0005240101820190>).

Lampiran Source Code Halaman Login

Source Code

```
from Tkinter import *
from random import randint
import tkFileDialog as fdialog
import tkMessageBox
import hashlib
import time
from xml.etree import ElementTree
import string
from xml.etree import ElementTree as ET
import sys
import datetime
import Tkinter, Tkconstants, tkFileDialog
import ttk
import socket
import uuid
from time import gmtime, strftime
class Login:
def __init__(self, parent, title):
    self.parent = parent
    w = 350
    h = 300
    ws = parent.winfo_screenwidth()
    hs = parent.winfo_screenheight()
    x = (ws/2) - (w/2)
    y = (hs/2) - (h/2)
    parent.geometry('%dx%d+%d+%d' % (w, h, x, y))
    self.parent.title(title)
    mainFrame = Frame(self.parent)
    mainFrame.pack(fill=BOTH, expand=YES)
    mainFrame2 = Frame(self.parent)
    mainFrame2.pack(fill=BOTH, expand=YES)
    ## Frame!
    leftFrame = Frame(mainFrame2, bd=10)
    leftFrame.pack(fill=BOTH, expand=YES, side=LEFT)
    leftBottomFrame = Frame(leftFrame, bd=10)
    leftBottomFrame.pack(fill=BOTH, expand=YES, side=BOTTOM)
    Label(leftBottomFrame, text='Please Insert').grid(row=0,
column=0, sticky=W)
    Label(leftBottomFrame, text='Username').grid(row=2, column=0,
sticky=W)
    self.userName = Entry(leftBottomFrame, width=20)
    self.userName.grid(row=2, column=1)
    Label(leftBottomFrame, text='Password').grid(row=3, column=0,
sticky=W)
    self.passwordName = Entry(leftBottomFrame, show = '*',
width=20)
    self.passwordName.grid(row=3, column=1)
    Label(leftBottomFrame, text='Password').grid(row=3, column=0,
sticky=W)
    self.passwordName = Entry(leftBottomFrame, show = '*',
width=20)
    self.passwordName.grid(row=3, column=1)
    btnAwal = Button(leftBottomFrame, text='Login', width=6,
command=self.checklogin)
    btnAwal.grid(row=4, column=1)
    filemenu = Menu(menuubar, tearoff=0)
```

```

filemenu.add_command(label="Add Files...")
filemenu.add_command(label="Add Folder...")
filemenu.add_separator()
filemenu.add_command(label="Exit")
menubar.add_cascade(label="File", menu=filemenu)
def checklogin(self):
    username = self.userName.get()
    password = self.passwordName.get()
    ip_fr = (socket.gethostbyname(socket.gethostname()))
    mac = ':'.join([':02x}'.format((uuid.getnode() >> i) & 0xff)
for i in range(0,8*6,8)][::-1])
    mzc = str(mac)
    file = open('RulesV2_1.xhtml','r')
    tree = ET.parse(file)
    root = tree.getroot()
    target =
root.find("{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Target")
    rule =
root.find("{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Rule")
    sub_target =
target.find("{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Subjects")
    sub_target2 =
rule.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Environmen
ts")
    sub_target3 =
rule.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Resources"
)
    sub_target4 =
rule.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Actions")
    ##env =
sub_target2.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Env
ironment")
    check_username1_fr = []
    check_username1_inv = []
    check_username1_off = []
    check_username1_law = []
    check_password1_fr = []
    check_password1_inv = []
    check_password1_off = []
    check_password1_law = []
    f_r = ""
    inv = ""
    off = ""
    law = ""
    check_env_fr = []
    check_env_inv = []
    check_env_off = []
    check_env_law = []
    check_env1_fr = []
    check_env1_inv = []
    check_env1_off = []
    check_env1_law = []
    count = 0
    for root2 in sub_target.getchildren():
        if count == 0:
            f_r = root2
        elif count == 1:
            inv = root2
        elif count == 2:
            off = root2
        elif count == 3:

```

```

        law = root2
        count += 1
    countx = 0
    for root22 in sub_target2.getchildren():
        if countx == 0:
            env_f_r = root22
        elif countx == 1:
            env_inv = root22
        elif countx == 2:
            env_off = root22
        elif countx == 3:
            env_law = root22
        countx += 1
    ## FR IP
    for root3_ipx in env_f_r.getchildren():
check_env_fr.append(root3_ipx.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}EnvironmentAttributeDesignator").attrib['Issuer'])
    try:
        check_env_fr.index(ip_fr)
    except:
        check_env1x = "none"
    else:
        check_env1x = "available"
    ## FR MAC
    for root33_ipx in env_f_r.getchildren():
check_env1_fr.append(root33_ipx.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}EnvironmentAttributeDesignator").attrib['Issuer'])
    try:
        check_env1_fr.index(mzc)
    except:
        check_env11x = "none"
    else:
        check_env11x = "available"
    ## FR
    for root3x in f_r.getchildren():
check_username1_fr.append(root3x.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}SubjectAttributeDesignator").attrib['Issuer'])
    try:
        check_username1_fr.index(username)
    except:
        check_username1x = "none"
    else:
        check_username1x = "available"
    for root3xx in f_r.getchildren():
check_password1_fr.append(root3xx.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}SubjectAttributeDesignator").attrib['Issuer'])
    try:
        check_password1_fr.index(password)
    except:
        check_password1x = "none"
    else:
        check_password1x = "available"
    ## INV IP
    for root4_ipx in env_inv.getchildren():
check_env_inv.append(root4_ipx.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}EnvironmentAttributeDesignator").attrib['Issuer'])
    try:
        check_env_inv.index(ip_fr)
    except:
        check_env2x = "none"
    else:

```

```

        check_env2x = "available"
        ## INV MAC
        for root44_ipx in env_inv.getchildren():
check_env1_inv.append(root44_ipx.find("://{urn:oasis:names:tc:xacml:2.0
:policy:schema:os}EnvironmentAttributeDesignator").attrib['Issuer'])
        try:
            check_env1_inv.index(mzc)
        except:
            check_env22x = "none"
        else:
            check_env22x = "available"
        ## Inv
        for root4x in inv.getchildren():
check_username1_inv.append(root4x.find("://{urn:oasis:names:tc:xacml:2.
0:policy:schema:os}SubjectAttributeDesignator").attrib['Issuer'])
        try:
            check_username1_inv.index(username)
        except:
            check_username2x = "none"
        else:
            check_username2x = "available"
            print check_username2x
        for root4xx in inv.getchildren():
check_password1_inv.append(root4xx.find("://{urn:oasis:names:tc:xacml:2
.0:policy:schema:os}SubjectAttributeDesignator").attrib['Issuer'])
        try:
            check_password1_inv.index(password)
        except:
            check_password2x = "none"
        else:
            check_password2x = "available"
        ## off IP
        for root5_ipx in env_off.getchildren():
check_env_off.append(root5_ipx.find("://{urn:oasis:names:tc:xacml:2.0:p
olicy:schema:os}EnvironmentAttributeDesignator").attrib['Issuer'])
        try:
            check_env_off.index(ip_fr)
        except:
            check_env3x = "none"
        else:
            check_env3x = "available"
        ## off MAC
        for root55_ipx in env_off.getchildren():
check_env1_off.append(root55_ipx.find("://{urn:oasis:names:tc:xacml:2.0
:policy:schema:os}EnvironmentAttributeDesignator").attrib['Issuer'])
        try:
            check_env1_off.index(mzc)
        except:
            check_env33x = "none"
        else:
            check_env33x = "available"
        ## Off
        for root5x in off.getchildren():
check_username1_off.append(root5x.find("://{urn:oasis:names:tc:xacml:2.
0:policy:schema:os}SubjectAttributeDesignator").attrib['Issuer'])
        try:
            check_username1_off.index(username)
        except:
            check_username3x = "none"
        else:
            check_username3x = "available"

```



```

    for root5xx in off.getchildren():
check_password1_off.append(root5xx.find("./{urn:oasis:names:tc:xacml:2.0:policy:schema:os}SubjectAttributeDesignator").attrib['Issuer'])
    try:
        check_password1_off.index(password)
    except:
        check_password3x = "none"
    else:
        check_password3x = "available"
    ## law IP
    for root6_ipx in env_law.getchildren():
check_env_law.append(root6_ipx.find("./{urn:oasis:names:tc:xacml:2.0:policy:schema:os}EnvironmentAttributeDesignator").attrib['Issuer'])
    try:
        check_env_law.index(ip_fr)
    except:
        check_env4x = "none"
    else:
        check_env4x = "available"
    ## law MAC
    for root66_ipx in env_law.getchildren():
check_env1_law.append(root66_ipx.find("./{urn:oasis:names:tc:xacml:2.0:policy:schema:os}EnvironmentAttributeDesignator").attrib['Issuer'])
    try:
        check_env1_law.index(mzc)
    except:
        check_env44x = "none"
    else:
        check_env44x = "available"
    ## law time
    for root77_ipx in env_law.getchildren():
        a =
root77_ipx.find("./{urn:oasis:names:tc:xacml:2.0:policy:schema:os}EnvironmentAttributeDesignator")
    ## law
    for root6x in law.getchildren():
check_username1_law.append(root6x.find("./{urn:oasis:names:tc:xacml:2.0:policy:schema:os}SubjectAttributeDesignator").attrib['Issuer'])
    try:
        check_username1_law.index(username)
    except:
        check_username4x = "none"
    else:
        check_username4x = "available"
    for root6xx in law.getchildren():
check_password1_law.append(root6xx.find("./{urn:oasis:names:tc:xacml:2.0:policy:schema:os}SubjectAttributeDesignator").attrib['Issuer'])
    try:
        check_password1_law.index(password)
    except:
        check_password4x = "none"
    else:
        check_password4x = "available"
    reso_fr = []
    act_fr = []
    reso_inv = []
    act_inv = []
    reso_off = []
    act_off = []
    reso_law = []
    act_law = []

```

```

        if check_username1x == "available" and check_password1x ==
"available":
            if check_env1x == "available" and check_env11x ==
"available":

sub_target3.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Res
ource")

sub_target4.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Act
ion")

        for rooty in sub_target3.getchildren():
            if
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceA
ttributeDesignator[@Issuer='Upload Digital Evidence']") is not None:
reso_fr.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sche
ma:os}ResourceAttributeDesignator").attrib['Issuer'])
                elif
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceA
ttributeDesignator[@Issuer='Create Cabinet']") is not None:
reso_fr.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sche
ma:os}ResourceAttributeDesignator").attrib['Issuer'])
                    elif
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceA
ttributeDesignator[@Issuer='Create Rack']") is not None:

reso_fr.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sche
ma:os}ResourceAttributeDesignator").attrib['Issuer'])
                        elif
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceA
ttributeDesignator[@Issuer='Create Bag']") is not None:
reso_fr.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sche
ma:os}ResourceAttributeDesignator").attrib['Issuer'])
                            elif
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceA
ttributeDesignator[@Issuer='Input Data Coc']") is not None:
reso_fr.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sche
ma:os}ResourceAttributeDesignator").attrib['Issuer'])
                                for roott in sub_target4.getchildren():
                                    if
roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAtt
ributeDesignator[@Issuer='Upload']") is not None:
act_fr.append(roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schem
a:os}ActionAttributeDesignator").attrib['Issuer'])
                                        elif
roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAtt
ributeDesignator[@Issuer='Create']") is not None:
act_fr.append(roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schem
a:os}ActionAttributeDesignator").attrib['Issuer'])
                                            elif
roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAtt
ributeDesignator[@Issuer='Input']") is not None:
act_fr.append(roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schem
a:os}ActionAttributeDesignator").attrib['Issuer'])
                                                tkMessageBox.showinfo("Info", "Welcome
!" + username + "\nYou Logged as First Responder\n\nResources:\n1.
" + reso_fr[0] + "\n2. " + reso_fr[1] + "\n3. " + reso_fr[2] + "\n4.
" + reso_fr[3] + "\n5. " + reso_fr[4] + "\nActions:\n1. " + act_fr[0] + "\n2.
" + act_fr[1] + "\n3. " + act_fr[2])
                                                    else:
tkMessageBox.showerror("Info", "Incorrect IP Address or
Mac Address!")

```

```

        elif check_username2x == "available" and check_password2x ==
"available":
            if check_env2x == "available" and check_env22x ==
"available":

sub_target3.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Res
ource")

sub_target4.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Act
ion")

        for rooty in sub_target3.getchildren():
            if
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceA
ttributeDesignator[@Issuer='Download Digital Evidence']") is not None:
reso_inv.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sch
ema:os}ResourceAttributeDesignator").attrib['Issuer'])
            elif
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceA
ttributeDesignator[@Issuer='Complete The Data Coc']") is not None:
reso_inv.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sch
ema:os}ResourceAttributeDesignator").attrib['Issuer'])
                for roott in sub_target4.getchildren():
                    if
roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAtt
ributeDesignator[@Issuer='Complete Data']") is not None:
act_inv.append(roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sche
ma:os}ActionAttributeDesignator").attrib['Issuer'])
                    elif
roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAtt
ributeDesignator[@Issuer='Download']") is not None:
act_inv.append(roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sche
ma:os}ActionAttributeDesignator").attrib['Issuer'])
                        tkMessageBox.showinfo("Info", "Welcome
!" + username + "\nYou Logged as Investigator\n\nResources:\n1.
" + reso_inv[0] + "\n2. " + reso_inv[1] + "\n\nActions:\n1. " + act_inv[0] + "\n2.
" + act_inv[1])
                    else:
                        tkMessageBox.showerror("Info", "Incorrect IP Address or
Mac Address!")
                elif check_username3x == "available" and check_password3x ==
"available":
                    if check_env3x == "available" and check_env33x ==
"available":

sub_target3.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Res
ource")

sub_target4.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Act
ion")

        for rooty in sub_target3.getchildren():
            if
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceA
ttributeDesignator[@Issuer='Delete Digital Evidence']") is not None:
reso_off.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sch
ema:os}ResourceAttributeDesignator").attrib['Issuer'])
            elif
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceA
ttributeDesignator[@Issuer='Change Password User']") is not None:
reso_off.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sch
ema:os}ResourceAttributeDesignator").attrib['Issuer'])

```

```

        elif
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Validate Digital Evidence']") is not None:
reso_off.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])
        elif
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Validate Status Case']") is not None:
reso_off.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])
        elif
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Download Form Coc']") is not None:
reso_off.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])
        elif
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Change Code Signature']") is not None:
reso_off.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])
        elif
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator[@Issuer='Validate Data Coc']") is not None:
reso_off.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceAttributeDesignator").attrib['Issuer'])
            for roott in sub_target4.getchildren():
                if
roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAttributeDesignator[@Issuer='Delete']") is not None:
act_off.append(roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAttributeDesignator").attrib['Issuer'])
                    if
roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAttributeDesignator[@Issuer='Change Password']") is not None:
act_off.append(roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAttributeDesignator").attrib['Issuer'])
                        elif
roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAttributeDesignator[@Issuer='Validate']") is not None:
act_off.append(roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAttributeDesignator").attrib['Issuer'])
                            elif
roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAttributeDesignator[@Issuer='Download Form']") is not None:
act_off.append(roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAttributeDesignator").attrib['Issuer'])
                                elif
roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAttributeDesignator[@Issuer='Change Code']") is not None:
act_off.append(roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAttributeDesignator").attrib['Issuer'])
                                    tkMessageBox.showinfo("Info", "Welcome
!"+username+"\nYou Logged as Officer\n\nResources:\n1.
"+reso_off[0]+" \n2. "+reso_off[1]+" \n3. "+reso_off[2]+" \n4.
"+reso_off[3]+" \n5. "+reso_off[4]+" \n6. "+reso_off[5]+" \n7.
"+reso_off[6]+" \n\nActions:\n1. "+act_off[0]+" \n2. "+act_off[1]+" \n3.
"+act_off[2]+" \n4. "+act_off[3]+" \n5. "+act_off[4])
                                        else:
                                            tkMessageBox.showerror("Info", "Incorrect IP Address or
Mac Address!")

```

```

elif check_username4x == "available" and check_password4x ==
"available":
    print "Ok Law"
    if check_env4x == "available" and check_env44x ==
"available":
        b = a.attrib['Issuer']
        spliter = b.split('-')
        now1 = strftime("%H:%M")
        if now1 > spliter[0] and now1 < spliter[1]:

sub_target3.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Res
ource")

sub_target4.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}Act
ion")

        for rooty in sub_target3.getchildren():
            if
rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ResourceA
ttributeDesignator[@Issuer='Download Form Coc']") is not None:
reso_law.append(rooty.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sch
ema:os}ResourceAttributeDesignator").attrib['Issuer'])
                for roott in sub_target4.getchildren():
                    if
roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:schema:os}ActionAtt
ributeDesignator[@Issuer='Download Form']") is not None:
act_law.append(roott.find(".//{urn:oasis:names:tc:xacml:2.0:policy:sche
ma:os}ActionAttributeDesignator").attrib['Issuer'])
                        tkMessageBox.showinfo("Info", "Welcome
!" + username + "\nYou Logged as Law\n\nResources:\n1.
" + reso_law[0] + "\n\nActions:\n1. " + act_law[0])
                                else:
                                    tkMessageBox.showerror("Info", "your access time is
not appropriate, You Can Login Between 09.00 - 15.00!")
                                        else:
                                            tkMessageBox.showerror("Info", "Incorrect IP Address or
Mac Address!")
                                                else:
                                                    tkMessageBox.showerror("Info", "Wrong Username or
Password!")
if __name__ == '__main__':
    root = Tk()
    menubar = Menu(root)
    aplikasi = Login(root, "Login System")
    root.config(menu=menubar)
    root.mainloop()

```

Lampiran XACML Policy

Policy
<pre> <?xml version="1.0" encoding="UTF-8"?> <Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" PolicyId="Access_Control_LPBD" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining- algorithm:first-applicable"> <Target> </pre>

```

<Subjects>
  <Subject>
    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
      <SubjectAttributeDesignator AttributeId="urn:xadl:subject"
DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="Institution_1" MustBePresent="true" />
    </SubjectMatch>
    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
      <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-format"
DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="fadlypanende" MustBePresent="true" />
    </SubjectMatch>
    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
      <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="fadly123" />
    </SubjectMatch>
  </Subject>
  <Subject>
    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
      <SubjectAttributeDesignator AttributeId="urn:xadl:subject"
DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="Institution_1" MustBePresent="true" />
    </SubjectMatch>

```

```

    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
    <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-format"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="santoso"
MustBePresent="true" />
    </SubjectMatch>
    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
    <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="santosol23"
MustBePresent="true" />
    </SubjectMatch>
</Subject>
<Subject>
    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
    <SubjectAttributeDesignator AttributeId="urn:xadl:subject"
DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="Institution_1" MustBePresent="true" />
    </SubjectMatch>
    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
    <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-format"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="dadang"
MustBePresent="true" />
    </SubjectMatch>

```

```

    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
    <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="dadang123"
/>
    </SubjectMatch>
</Subject>
<Subject>
    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
    <SubjectAttributeDesignator AttributeId="urn:xadl:subject"
DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="Institution_1" MustBePresent="true" />
    </SubjectMatch>
    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
    <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:name-format"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="hotman"
MustBePresent="true" />
    </SubjectMatch>
    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:assignUser</AttributeValue>
    <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="hotman123"
MustBePresent="true" />
    </SubjectMatch>

```



```

    </Subject>
  </Subjects>
  <Resources>
    <Resource>
      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Upload File Digital
Evidence</AttributeValue>
      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Upload
Digital Evidence" MustBePresent="true" />
      </ResourceMatch>
    </Resource>
    <Resource>
      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Create New
Cabinet</AttributeValue>
      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Crate
Cabinet" MustBePresent="true" />
      </ResourceMatch>
    </Resource>
    <Resource>
      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Create New
Rack</AttributeValue>
      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Create Rack"
MustBePresent="true" />
      </ResourceMatch>
    </Resource>
  </Resources>

```

```

    <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Create New
Bag</AttributeValue>
    <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Create Bag"
MustBePresent="true" />
    </ResourceMatch>
</Resource>
<Resource>
    <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Input File Data Case
Coc</AttributeValue>
    <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Input Data
Case Coc" MustBePresent="true" />
    </ResourceMatch>
</Resource>
<Resource>
    <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Download File
Digital Evidence</AttributeValue>
    <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download
Digital Evidence" MustBePresent="true" />
    </ResourceMatch>
</Resource>
<Resource>
    <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Complete File Data
Coc</AttributeValue>

```

```

        <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Complete The
Data Coc" MustBePresent="true" />
    </ResourceMatch>
</Resource>
<Resource>
    <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Delete File Digital
Evidence</AttributeValue>
        <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Delete
Digital Evidence" MustBePresent="true" />
    </ResourceMatch>
</Resource>
<Resource>
    <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Change Password All
User</AttributeValue>
        <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Change
Password User" MustBePresent="true" />
    </ResourceMatch>
</Resource>
<Resource>
    <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Validate File
Digital Evidence</AttributeValue>
        <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Validate
Digital Evidence" MustBePresent="true" />
    </ResourceMatch>

```

```

    </Resource>
    <Resource>
      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Validate File Case
Status</AttributeValue>
      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Validate
Case Status" MustBePresent="true" />
      </ResourceMatch>
    </Resource>
    <Resource>
      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Download File Form
Coc</AttributeValue>
      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download
Form Coc" MustBePresent="true" />
      </ResourceMatch>
    </Resource>
    <Resource>
      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Change File Code
Signature</AttributeValue>
      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Change Code
Signature" MustBePresent="true" />
      </ResourceMatch>
    </Resource>
    <Resource>
      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">

```

```

        <AttributeValue
DataTyPe="http://www.w3.org/2001/XMLSchema#string">Validate File Data
Coc</AttributeValue>

        <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataTyPe="http://www.w3.org/2001/XMLSchema#string" Issuer="Validate
Data Coc" MustBePresent="true" />
        </ResourceMatch>
    </Resource>
</Resources>
</Target>
<Rule Effect="Permit" RuleId="Rules">
    <Target>
        <Subjects>
            <Subject>
                <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue
DataTyPe="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:addRole</AttributeValue>
                    <SubjectAttributeDesignator
AttributeId="urn:xadl:subject:dst"
DataTyPe="http://www.w3.org/2001/XMLSchema#string" Issuer="First
Responder" MustBePresent="true" />
                    </SubjectMatch>
                </Subject>
                <Subject>
                    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <AttributeValue
DataTyPe="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:addRole</AttributeValue>
                        <SubjectAttributeDesignator
AttributeId="urn:xadl:subject:src"
DataTyPe="http://www.w3.org/2001/XMLSchema#string"
Issuer="Investigator" MustBePresent="true" />
                        </SubjectMatch>
                    </Subject>
                <Subject>
                    <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">

```

```

        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:addRole</AttributeValue>
        <SubjectAttributeDesignator
AttributeId="urn:xadl:subject:src"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Officer"
MustBePresent="true" />
        </SubjectMatch>
    </Subject>
    <Subject>
        <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:xadl:action:rbac
:addRole</AttributeValue>
            <SubjectAttributeDesignator
AttributeId="urn:xadl:subject:src"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Lawyer"
MustBePresent="true" />
            </SubjectMatch>
        </Subject>
    </Subjects>
    <Resources>
        <Resource>
            <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Upload File Digital
Evidence</AttributeValue>
                <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Upload
Digital Evidence" MustBePresent="true" />
                </ResourceMatch>
            </Resource>
        <Resource>
            <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Create New
Cabinet</AttributeValue>

```

```

        <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Create
Cabinet" MustBePresent="true" />
        </ResourceMatch>
    </Resource>
    <Resource>
        <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Create New
Rack</AttributeValue>
                <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Create Rack"
MustBePresent="true" />
                    </ResourceMatch>
                </Resource>
                <Resource>
                    <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Create New
Bag</AttributeValue>
                            <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Create Bag"
MustBePresent="true" />
                                </ResourceMatch>
                            </Resource>
                            <Resource>
                                <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                                    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Input Data Case
Coc</AttributeValue>
                                        <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Input Data
Coc" />
                                            </ResourceMatch>
                                        </ResourceMatch>
                                    </Resource>
                                </Resource>
                            </Resource>
                    </ResourceMatch>
                </Resource>
            </ResourceMatch>
        </Resource>
    </Resource>

```

```

    </Resource>
    <Resource>
      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Download File
Digital Evidence</AttributeValue>
      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download
Digital Evidence" MustBePresent="true" />
      </ResourceMatch>
    </Resource>
    <Resource>
      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Complete File Data
Coc</AttributeValue>
      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Complete The
Data Coc" MustBePresent="true" />
      </ResourceMatch>
    </Resource>
    <Resource>
      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Delete File Digital
Evidence</AttributeValue>
      <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Delete
Digital Evidence" />
      </ResourceMatch>
    </Resource>
    <Resource>
      <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">

```



```

        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Change Password All
User</AttributeValue>
        <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Change
Password User" MustBePresent="true" />
        </ResourceMatch>
</Resource>
<Resource>
        <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Validate File
Digital Evidence</AttributeValue>
        <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Validate
Digital Evidence" MustBePresent="true" />
        </ResourceMatch>
</Resource>
<Resource>
        <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Validate Status File
Case</AttributeValue>
        <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Validate
Status Case" MustBePresent="true" />
        </ResourceMatch>
</Resource>
<Resource>
        <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Download File Form
Coc</AttributeValue>
        <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"

```

```

DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download
Form Coc" MustBePresent="true" />
    </ResourceMatch>
</Resource>
<Resource>
    <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Change Code File
Signature</AttributeValue>
    <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Change Code
Signature" MustBePresent="true" />
    </ResourceMatch>
</Resource>
<Resource>
    <ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Validate Data File
Coc</AttributeValue>
    <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Validate
Data Coc" MustBePresent="true" />
    </ResourceMatch>
</Resource>
</Resources>
<Actions>
    <Action>
        <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Upload</AttributeVal
ue>
        <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Upload" />
        </ActionMatch>
    </Action>

```

```

    <Action>
      <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Create Cabinet,
Rack, Bag</AttributeValue>
        <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Create"
MustBePresent="true" />
        </ActionMatch>
      </Action>
    <Action>
      <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Input
Data</AttributeValue>
        <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Input"
MustBePresent="true" />
        </ActionMatch>
      </Action>
    <Action>
      <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Download
File</AttributeValue>
        <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download"
MustBePresent="true" />
        </ActionMatch>
      </Action>
    <Action>
      <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">

```

```

        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Complete</AttributeV
alue>

        <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Complete
Data" MustBePresent="true" />
        </ActionMatch>
    </Action>
    <Action>
        <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Delete
File</AttributeValue>
            <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Delete"
MustBePresent="true" />
            </ActionMatch>
        </Action>
    <Action>
        <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Change Password
User</AttributeValue>
            <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Change
Password" MustBePresent="true" />
            </ActionMatch>
        </Action>
    <Action>
        <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Validate File,
Status, Data</AttributeValue>
            <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"

```

```

DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Validate"
MustBePresent="true" />
    </ActionMatch>
</Action>
<Action>
    <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Download</AttributeV
alue>
    <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Download
Form" MustBePresent="true" />
    </ActionMatch>
</Action>
<Action>
    <ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">Change Code
Signature</AttributeValue>
    <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="Change Code"
MustBePresent="true" />
    </ActionMatch>
</Action>
</Actions>
<Environments>
    <Environment>
        <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
        <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authn-locality:ip-
address" DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="10.100.53.198" MustBePresent="true" />
        </EnvironmentMatch>

```

```

    <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
    <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:key-info"
DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="c4:b3:01:ba:5f:79" MustBePresent="true" />
    </EnvironmentMatch>
    <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
    <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="24"
MustBePresent="true" />
    </EnvironmentMatch>
</Environment>
<Environment>
    <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
    <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authn-locality:ip-
address" DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="10.100.53.198" MustBePresent="true" />
    </EnvironmentMatch>
    <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
    <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:key-info"
DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="c4:b3:01:ba:5f:79" MustBePresent="true" />

```

```

        </EnvironmentMatch>
        <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
            <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="24"
MustBePresent="true" />
            </EnvironmentMatch>
        </Environment>
    <Environment>
        <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
            <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authn-locality:ip-
address" DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="10.100.53.198" MustBePresent="true" />
            </EnvironmentMatch>
        <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
            <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:key-info"
DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="c4:b3:01:ba:5f:79" MustBePresent="true" />
            </EnvironmentMatch>
        <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
            <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"

```

```

    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="24"
    MustBePresent="true" />
        </EnvironmentMatch>
    </Environment>
    <Environment>
        <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
                <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authn-locality:ip-
address" DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="10.100.53.198" MustBePresent="true" />
                    </EnvironmentMatch>
                <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
                        <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:key-info"
DataType="http://www.w3.org/2001/XMLSchema#string"
Issuer="c4:b3:01:ba:5f:79" MustBePresent="true" />
                            </EnvironmentMatch>
                        <EnvironmentMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:x
acml:2.0:actions:enableRole</AttributeValue>
                                <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="09.00-15.00"
/>
                                    </EnvironmentMatch>
                                </Environment>
                            </Environments>
                        </Target>
                    </Rule>
                </Policy>

```