KONSEP *ATTRIBUTE BASED ACCESS CONTROL* (ABAC) PADA LEMARI PENYIMPANAN BUKTI DIGITAL (LPBD)

Moh. Fadly Panende[1], Yudi Prayudi[2], Imam Riadi[3]

[1,2] Program Studi Magister Teknik Informatika, Universitas Islam Indonesia
[3]Program Studi Sistem Informasi, Universitas Ahmad Dahlan Yogyakarta
[1]fadlypanende@gmail.com, [2]prayudi@uii.ac.id, [3]imam.riadi@is.uad.ac.id

ABSTRAK

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. Sistem lemari penyimpanan bukti digital (LPBD) menjadi salah satu solusi untuk permasalahan manajemen bukti digital yang berdasar pada *digital evidence cabinet* (DEC), hanya saja sistem tersebut belum dilengkapi dengan model *access control* yang baik. *Access control* yang terapkan terhadap LPBD sebelumnya dibuat hanya dengan mekanisme otentikasi dan otorisasi *username* dan *password* saja, tidak adanya parameter lain yang lebih kompleks untuk mendukung sebuah *request* pada sistem LPBD. Tujuan dilakukannya penelitian ini yaitu membuat model *attribute based access control* (ABAC) dan melakukan pengujian terhadap *access control* yang dibuat. Berdasarkan hasil pengujian ABAC yang dilakukan menggunakan *tools* yang dibuat khusus untuk menguji ABAC pada LPBD, bahwa *access control* dapat berjalan dengan baik dan berfungsi sebagaimana mestinya. Perancangan ABAC LPBD ini juga diharapkan dapat menjadi solusi terhadap permasalahan yang ada pada *access control* LPBD sebelumnya. Pendekatan menggunakan metode ABAC ini disebabkan ABAC merupakan model *access control* yang lebih fleksibel dalam penerapan *attribute* terhadap *user*, dan hierarchy XACML yang dapat mendukung kebutuhan *access control* yang digunakan pada LPBD.

Kata Kunci: *Access Control, ABAC, XACML, LPBD.DEC*

ABSTRACT

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. The digital evidence storage cabinet (LPBD) system is one of the solutions to digital evidence management problems based on digital evidence cabinet (DEC), only that the system is not equipped with a good access control model. The access control applied to the previous LPBD was created only with athentication mechanism and authorization of username and password only, no other more complex parameters to support a request on the LPBD system. The purpose of this research is to create an attribute model based access control (ABAC) and to test the access control that is made. Based on ABAC test results conducted using tools specially designed to test ABAC on LPBD, that access control can run well and function. The design of ABAC is also expected to be a solution to the problems that exist onthe LPBD access control before. The ABAC method approach is because ABAC is a more flexible access control model in the application of attribute to user. XACML hierarchy can support access control requirement used in LPBD.

Keywords: *Access Controls, ABAC, XACML, LPBD, DEC.*

DOI: 10.15408/jti.v11i1.7220

I. PENDAHULUAN

Perkembangan teknologi informasi saat ini tidak hanya memberikan dampak positif bagi penggunanya, melainkan juga dampak negatif, Berdasarkan data dari Polda Metro Jaya terdapat 1.207 kasus *cybercrime* pada tahun 2016 dengan 699 kasus yang terselesaikan. Data ini menjukan bahwa *cybercrime* sudah menjadi permasalahan yang serius di era digital ini.

Salah satu faktor penting dalam proses investigasi sebuah kasus *cybercrime* yaitu hal yang terkait dengan barang bukti [1], 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, *hardisk*, dan lain-lain) sedangkan bukti digital adalah barang bukti yang berisi informasi-informasi digital hasil ekstaksi dari bukti elektronik. Bukti digital merupakan alat bukti yang sah dipengadilan, sebagaimana yang dijelaskan oleh [2] 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". Penanganan bukti digital dapat menjadi bukti adanya tekad bahwa kejahatan telah dilakukan atau mungkin memberikan hubungan antara kejahatan dan korban atau kejahatan dan pelakunya [3]. Dalam proses menyelidiki kasus kejahatan digital, bukti digital diperlukan untuk menyelesaikan kasus-kasus yang ada [4]. 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 yang terus berkembang dan semakin kompleks maka muncullah salah satu solusi yang ditawarkan [5] yaitu model *digital evidence cabinets* sebagai pendekatan baru yang diimplementasikan dalam penanganan bukti digital dan *chain of custody*. Solusi ini diorentasikan untuk memberikan penyelesaian masalah penyimpanan bukti digital. Model tersebut telah diimplementasikan [6] 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 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) dan lain-lain, 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.

Access Control terhadap LPBD tidak cukup hanya ditangani oleh mekanisme otentifikasi dan otorisasi *user* saja. Otentifikasi, otorisasi dan *access control* memiliki fungsi dan tujuan yang berbeda walaupun pada implementasinya seolah-olah terlihat sebuah proses tunggal. Menurut [7] otentifikasi fokusnya pada verifikasi terhadap klaim identitas *user*, otorisasi fokusnya pada pemberian hak akses terhadap *resource*, sementara *access control* fokusnya pada proteksi keamanan yang diterapkan. Akses kontrol melindungi sistem dan sumber daya dari akses yang tidak berhak dan menentukan tingkat otorisasi setelah prosedur otentifikasi berhasil dilengkapi [8].

Mengingat belum adanya skema rancangan model akses kontrol yang baik pada LPBD ini, maka perlu dilakukan perancangan model akses kontrol *policy* menggunakan pendekatan *attribute based access control* (ABAC) yang mendukung kebutuhan Lemari Penyimpanan Bukti Digital (LPBD) itu sendiri. Hasil akhir dari penelitian ini adalah

terciptanya model *attribute based access control policy* untuk memberikan hak akses bagi pengguna yang diberi kewenangan menangani bukti digital yang ada pada LPBD

II. TINJAUAN PUSTAKA

dari bagian-bagian yang berhubungan langsung dengan bukti digital, penyimpanan informasi metadata bukti digital maupun kontrol akses dan kemananan terhadap digital CoC [6]. Konsep ini diperkenalkan oleh [9] dalam penelitiannya yang berjudul *Digital Evidence Cabinets : A Proposed Frameworks for Handling Digital Chain of Custody.* Dalam penelitiannya disebutkan bahwa LPBD 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. Penelitian yang dilakukan oleh [10] dikatakan bahwa Peran artefak (misalnya metadata) dalam analisis forensik dan (prospektif) adalah hilangnya artefak ini saat data dikumpulkan dari lingkungan komputasi awan. Jika metadata (misal: tanggal pembuatan/modifikasi dari sebuah file, dan mencatat kepemilikan pengguna) yang hilang selama proses pengumpulan. Ini mempengaruhi kemampuan peneliti untuk melakukan penyelidikan forensik terhadap standar yang disyaratkan oleh pengadilan. Penelitian lain yang dilakukan oleh [11] menawarkan metode solusi perlindungan bagi pengguna dalam aplikasi *browser* yang akan difilter, menonaktifkan *plugin*, memberi tahu, memblokir, dan mengurangi serangan *Cross Site Scripting.*

ABAC adalah sebuah metode *acces control* dimana *subject* hanya akan dapat melakukan *request* untuk menjalankan sebuah operasi terhadap *object* didasarkan pada *attribute* yang disematkan pada subjek, objek, kondisi lingkungan serta kumpulan *policy* yang termasuk dalam *attribute* dan kondisinya. Pada sistem ABAC, elemen otorisasi didefinisikan dalam terminologi *attribute. Attribute* itu sendiri adalah karakteristik dari entitas yang didefinisikan sebelumnya oleh pihak yang memiliki wewenang untuk itu. Menurut [12] ide dasar utama dari ABAC adalah tidak memberikan *permission* sebagai *ouput* dari hubungan langsung antara subjek dan objek namun mendasari pemberian *permission* tersebut melalui *attribute* dari keduanya.

Menurut [13], terdapat 4 aspek *attribute* dalam ABAC, yaitu*:*

1. *S*

   ubject adalah pengguna manusia ataupun non manusia misalnya (*device* ataupun komponen *software*) yang meminta *request access*. Contoh dari *attribute* 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.
2. *R*

   esource adalah sesuatu target yang dilindungi seperti halnya *device*, *files*, *record*, *table*, proses, program, jaringan.
3. *A*

   ctions 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*.
4. *E*

   nvironment attribute adalah karakteristik dari operational ataupun situational seperti misalnya *current time, current temperature, IP address*.

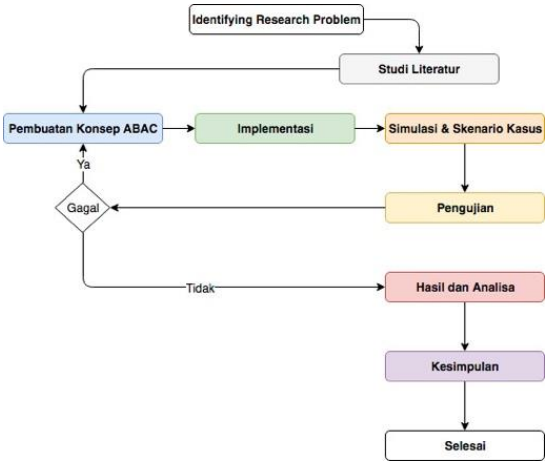
Penelitian yang dilakukan oleh [14] yang menyajikan permasalahan sistem kontrol akses lintas domain ABAC bersama dengan domain keamanan sebagai *attribute* dengan subjek, objek, otoritas, *attribute* lingkungan sebagai dasar akses untuk akses pengambilan keputusan. Penelitian selanjutnya yang dilakukan oleh [15] 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 *subject*, lingkungan dan sumberdaya untuk petmintaan menulis ulang.

XACML (*eXtensible Access Control Markup Language*) adalah standar dari OASIS untuk menspesifikasikan ABAC *policy* menggunakan format XML. Terdapat 4

attribute predefined yaitu*: subject, resource, action dan environment*. Namun *type user attribute* dapat juga diterapkan untuk aplikasi tertentu. XACML mendukung berbagai *type* data, *type* nama serta *path expression* untuk *attribute* misalnya*: string*, *integer*, *internet-based names*, *regular expression* dan XPATH. Dalam hal penggunaan *attribute*, *type* data lebih utama dispesifikasikan dibandingkan dengan domain [16].

III. METODOLOGI

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 1.

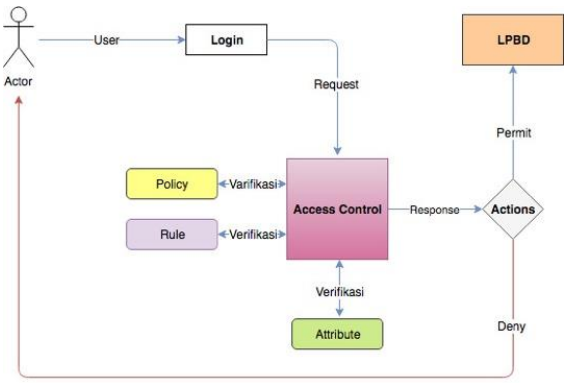


Gambar 1. Alur penelitian

Gambar 1 menjelaskan bahwa alur penelitian yang digunakan dalam penelitian ini adalah, diawali dengan *identifying research problem*, dilanjutkan dengan studi literatur untuk mendapatkan referensi-referensi tentang penelitian sebelumnya, selanjutnya membuat konsep ABAC, implementasi, melakukan simulasi dan skenario kasus, melakukan pengujian ABAC, jika pengujian gagal maka akan kembali ke perancangan konsep ABAC jika pengujian berhasil maka akan dilanjutkan pada hasil dan analisa, dan yang terakhir menyimpulkan hasil penelitian.

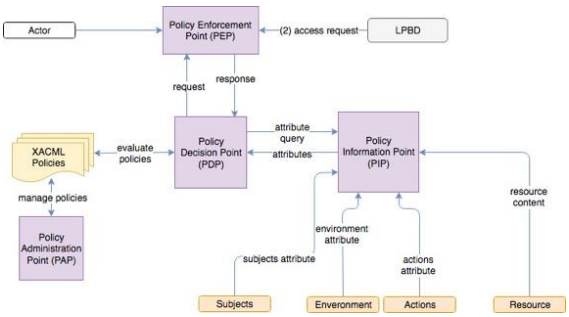
IV. GAMBARAN RANCANGAN *ACCESS CONTROL* LPBD

Perancangan konsep model *attribute based access control* (ABAC) ini dimulai dengan gambaran umum cara kerja akses kontrol yang dibangun. Rancangan ABAC pada LPBD ini dianalogikan sebagai sebuah proses *login* yang dimana proses otentifikasi dan autorisasinya dilakukan melalui *rule policy* yang disematkan pada setiap *user* yang memiliki hak akses pada LPBD sebagai *subject* dan *resource* pada aplikasi sebagai *object*. Rancangan *access control* ini dibuat agar dapat mengidentifikasi setiap *user* yang mengakses aplikasi dikarenakan LPBD merupakan sebuah aplikasi yang bersentuhan langsung dengan metadata bukti digital yang harus tetap terjaga keaslianya agar dapat dipertanggungjawabkan di pengadilan [1]. Gambar 3 menjelaskan tentang umum ABAC pada LPBD.



Gambar 2. Gambaran umum ABAC LPBD

XACML LPBD *data flow model* merupakan gambaran logika yang terlibat dalam melakukan pemrosesan terhadap sebuah permintaan akses. Gambar 3 menjelaskan model XACML *data flow* LPBD.



Gambar 3. XACML *data flow* LPBD

Gambar 3 menjelaskan bahwa *policy enfronce point* (PEP) sebagai pelaksana awal ketika dilakukannya permintaan akses, selanjutnya yang memberikan *request* terhadap *policy decision point* (PDP) yang bertugas sebagai yang memutuskan permintaan, dan

policy information point (PIP) yang berperan sebagai yang menampung 4 jenis *attribute* yaitu *subject*, *resource*, *actions*, dan *environment*. *Policy decision point* (PDP) dalam hal ini berfungsi untuk mengevaluasi XACML *policies* yang berada pada *policy administration point* (PAP) yang berfungsi sebagai yang mengolah XACML *policy* tersebut.

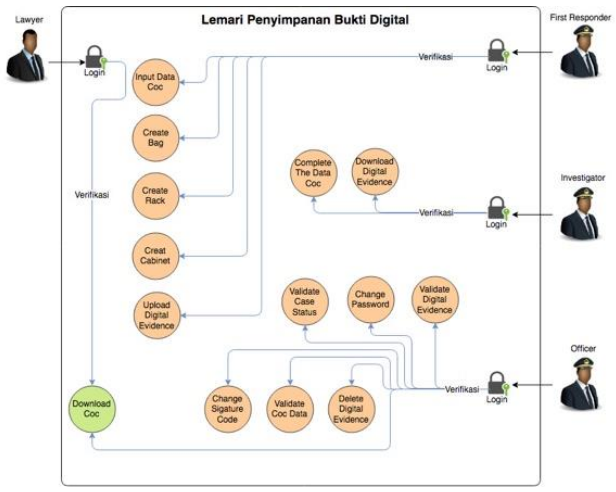
V. HASIL DAN PEMBAHASAN

Policy statement merupakan tahapan awal pada perancangan *access control* LPBD ini, yaitu berupa usulan *attribute* yang akan digunakan dan telah disesuaikan dengan kebutuhan-kebutuhan yang ada pada istem LPBD dan kebutuhan-kebutuhan yang ada pada ABAC. Tabel 1 merupakan penjelasan tentang usulan *attribute* pada sistem LPBD.

Tabel 1. Usulan attribute

Subject	***Resource***	***Actions***	***Environment***
First Responder	*Upload Digital Evidence*	*Upload*	*Ip Address Mac Addres Time Akses*
	Create Cabinet	*Create*	
	Create Rack	*Create*	
	Create Bag	*Create*	
	Input Data Case Coc	*Input*	
Investigator	*Download Digital Evidence*	*Download*	*Ip Address Mac Addres Time Akses*
	Complete The Data Coc	*Complete Data*	
Officer	*Delete Digital Evidence*	*Delete*	*Ip Address Mac Addres Time Akses*
	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*	
Layer	*Download Form Coc*	*Download*	*Ip Address Mac Addres Time Akses*

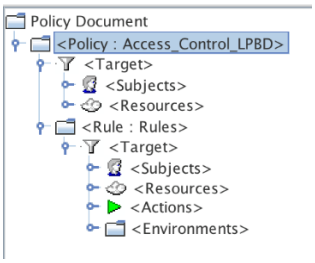
Tabel 1 menjelaskan bahwa dalam sebuah *policy statement* yang dibangun pada sistem LPBD berisi empat buah *subject* yang merupakan jabatan *user* yaitu *first responder*, *investigator*, *officer*, dan lawyer, lima belas buah *resource* sebagai *object* yaitu, *upload* digital, sembilan buah *actions*, dan tiga buah *evinronment* yang merupakan kondisi lingkungan saat *request* dilakukan, *subject* yang pertama yaitu *first responder* mempunyai hak melakukan operasi pada *resource*: *upload digital evidence, create cabinet, create rack, create bag*, dan *input data case coc*, serta *actions*: *upload, create, dan input. Environment* yang digunakan yaitu *ip address, mac address, dan time access*. *Subject* yang kedua yaitu *investigator* memeiliki dua hak akses pada *resource* yaitu *download digital evidence* dan *complete the data coc*, *actions*: *download* dan *complete data* serta *environment*: *ip address, mac address*, dan time *access*. *Subject* yang ketiga yaitu *officer* memiliki hak akses pada *resource*: *delete digital evidence, change password user, validate digital evidence, validate cese status, download form coc, change code signature*, dan *validate data coc*. *Actions* yang dimiliki yaitu *delete, change password, validate, download*, dan *change code*. *Environment*: *ip address*, *mac address*, dan *time access*. *Subject* yang keempat yaitu *lawyer* hanya memiliki satu hak akses *resource* yaitu *download form coc*, dan *action*: *download*, serta *inveronment*: *ip address, mac address dan time access*. *Policy statement* ini merupakan komponen-komponen yang akan dimasukan kedalam *rules* dan akan menjadi ekspresi logika untuk memenuhi setiap *request* yang dilakukan oleh *user*. Sebagaimana yang terlihat pada Gambar 4.



Gambar 4. *Policy statement*

Struktur XACML *policy* yang dibangun berdasarkan kebutuhan-kebutuhan yang ada

pada LPBD, serta dirancang menggunakan *tools* khusus untuk membuat sebuah XACML *policy*. *Tools* yang digunakan yaitu UMU-XACML-Editor Versi 1.3.2 Proses pembuatan *policy* terbagi atas dua bagian yaitu menentukan satu *policy* target serta satu *rule* hal ini bertujuan agar dapat dengan mudah menempatkan *attribute* yang akan disematkan pada setiap elemen yang ada seperti *subject*, *resource*, *actions*, dan *environment*. Berikut adalah *sample* pembuatan struktur XACML *policy* LPBD. Gambar 5 menjelaskan tentang XACML *policy* yang dibuat menggunakan UMU XACML Editor.



Gambar 5. XACML *policy* UMU XACML editor

Gambar 5 menjelaskan bahwa langkah pertama yang dilakukan yaitu menentukan nilai pada *policy* target yang juga merupakan *root element* pada rancangan XACML *policy* ini, *policyid* diberinama *access control policy LPBD* dan *rule combining algorithm* diisi dengan nilai *first applicable* hal ini bertujuan karena *policy* LPBD mempunyai *request* lebih dari 1 *rule*. *Target policy* berisi 4 *subject* yang artinya bahwa ada 4 *user* yang diizinkan melakukan pada LPBD yaitu *first responder*, *investigator*, *officer*, dan *lawyer*. Selain *subject*, *target policy* juga berisi 15 *resource* yang artinya merupakan jumlah keseluruhan *resource* yang ada pada LPBD.

Setelah menjelaskan bagaimana perancangan dilakukan maka langkah selanjutnya yaitu menjelaskan *sample output* dari rancangan XACML *policy* yang telah dibuat. Gambar 6 menjelaskan tentang *sample output attribute subject.*

```
- <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="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>
</Subjects>
```

Gambar 6. *Sample output subject*

Gambar 6 menjelaskan bahwa *sample attribute subject* yang ditampilkan adalah *output subject* dari *user first responder* yang artinya sample *subject* ini berisi *attribute* jabatan yang diisi dengan nama *first responder*, *username* diisi dengan *fadlypanende* dan *subjectId* diisi dengan *fadly123* yang artinya bahwa seseorang yang melakukan akses pada LPBD yaitu *user* yang menjabat sebagai *first responder* bernama *fadlypanende* dan *password fadly123.*

Gambar 7 menjelaskan *output sample atttribute resource.*

```
<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 7. *Sample output resource*

Gambar 7 menjelaskan bahwa *sample attribute resource* yang ditampilkan pada Gambar 7 merupakan *sample attribute resource* yang diberikan pada *user first responder* yang artinya bahwa seseorang yang memiliki wewenang sebagai *first responder* dapat diberikan izin melakukan akses pada LPBD atas dasar identitas *resource* yang diberikan berupa *upload file digital evidence, create new cabinet, create new rack, create new bag*, dan *input data coc.*

Tahapan selanjutnya menjelaskan *sample attribute output actions* sebagaimana yang terlihat pada Gambar 8.

```
<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 8. *Sample output actions*

Gambar 8 menjelaskan bahwa *output sample attribute actions* yang ditampilkan pada Gambar 8 merupakan *sample attribute actions* yang diberikan pada *user first responder* yang artinya bahwa seseorang yang memiliki kewenangan sebagai *first responder* dapat diberikan izin melakukan akses pada LPBD atas dasar identitas *actions* yang diberikan berupa *upload file, create cabinet, rack, bag* dan *input data.*

Tahapan akhir dari penjelasan *sample output* XACML *policy* ini yaitu *sample output attribute environment* sebagaimana yang terlihat pada Gambar 9.

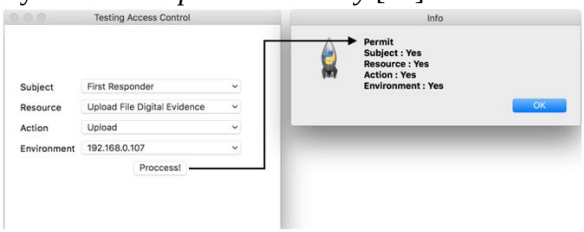
```
<Environments>
  <Environment>
    <EnvironmentMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">urn:oasis:names:tc:xacml:2.0:actions:enableRole</AttributeValue>
      <EnvironmentAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authn-locality:ip-a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


Gambar 9. *Sample output environment*

Gambar 9 menjelaskan bahwa *sample output attribute environment* yang ditampilkan pada Gambar 9 merupakan *sample attribute environment* yang diberikan pada *user first*

responder yang artinya bahwa seseorang yang memiliki kewenangan sebagai *first responder* dapat melakukan akses pada LPBD atas dasar identitas *attribute environment* yang diberikan berupa *ip address: 192.168.0.107, time access: 24* atau tidak ada batasan waktu akses, *dan mac address: c4:b3:01:ba:5f:79.*

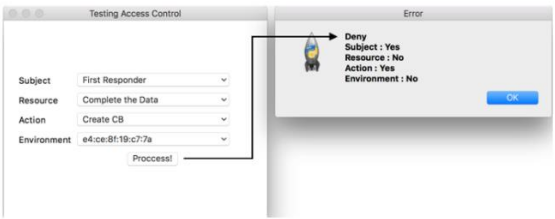
Aktivitas pengujian *access control* LPBD dilakukan menggunakan sebuah *tools* yang dibuat khusus untuk menguji kinerja *access control* yang dibuat pada LPBD. Pengujian yang ditampilkan menggunakan *tools testing access control* ini menggunakan 1 *sample* kondisi *permit* dan 1 *sample* kondisi *deny* serta *user first responder*, karena pada dasarnya hanya ada dua kemungkinan *decision* ketika *subject* melakukan *request* terhadap *object* yaitu kondisi *permit* dan *deny* [17].



Gambar 10. Pengujian kondisi *permit*

Gambar 10 menjelaskan bahwa pengujian kodisi *permit* terjadi ketika melakukan "klik" tombol *process* maka kondisi yang dihasilkan yaitu *permit* disebabkan semua *attribute* yang dimasukan benar, seperti yang terlihat pada halaman info *permit subject: yes,resource: yes, actions: yes* dan *environment:yes. Attribute* yang dimasukan yaitu *subject: first responder, resource: upload file digital evidence, actions: upload,* dan *environment: ip address 192.168.0.107.*

Selanjutnya melakukan pengujian kondisi *deny.* Gambar 11 menjelaskan kondisi *deny.*



Gambar 11. Pengujian kondisi *deny*

Gambar 11 menjelaskan bahwa sample pengujian kondisi *deny* menggunakan *user first responder,* ketika melakukan "klik" tombol *process* kondisi yang dihasilkan adalah *deny* sebagaimana yang terlihat pada halaman info *deny* bahwa *subject: yes, resource: no, actions: yes, environment: no,* terdapat 2 kesalahan yaitu pertama terdapat pada masukan *resource* yang diisi dengan *complete the data* dan kesalahan kedua terdapat pada masukan *environment* yang diisi dengan *e4:ce:8f:19:c7:7a* hal ini disebabkan bahwa *attribute resource* dan *environment* yang dimasukan bukan merupakan *attribute user first responder* melainkan *attribute user investigator.*

Aktivitas pengujian *access control* yang dilakukan pada LPBD ini merupakan pengujian fungsionalitas yang meliputi kemampuan menerapkan *rule policy* untuk proses *login* pada sistem LPBD.

Tabel 2 berikut merupakan penjelasan mengenai hasil pengujian 1 *sample* kondisi *permit* dan 1 *sample* kondisi *deny.*

Tabel 2 Hasil pengujian kondisi permit & deny

Subject	***Resource***	***Actions***	***Environment***	***Output***
First Responder	*Upload File Digital Evidence*	*Upload*	***I**p Address: 192.168.0.107*	*Permit*
First Responder	*Complete The Data*	*Create CB*	*Mac Address: e4:ce:8f:19:c7:7a*	*Deny*

Tabel 2 menjelaskan bahwa pengujian kondisi *permit* dan *deny* mendapatkan satu kondisi *permit* yang disebabkan keseluruhan *attribute* yang dimasukkan merupakan *attribute* yang telah disematkan pada *user* yaitu *subject first responder, resource: upload bukti digital, actions: upload* dan *environment: address 192.168.0.107.* Sementara kondisi *deny* disebabkan karena ada dua kesalahan masukan *attribute* yaitu *attribute resource: complete the data* dan *attribute* e*nvironment: mac address e4:ce:8f:19:c7:7a* yang bukan merupakan *attribute* yang ada pada *user first responder.*

Pengujian *access control* LPBD sebagaimana yang terlilhat pada Tabel 3 merupakan hasil pengujian *access control* menggunakan keselurahan *attribute* pada 4 *user* yaitu *first responder, investigator, officer,* dan *lawyer* yang divisualisasikan dalam bentuk tabel berisi hasil pengujian yang dilakukan menggunakan *tools testing access control* LPBD. Pengujian ini dilakukan agar dapat mengetahui bagaimana hasil kinerja *access control* secara keseluruhan dalam penerapan *attribute subject, resource, actions,* dan *environment* yang disematkan pada *user.* Tabel

3 menjelaskan tentang hasil pengujian secara keseluruhan *attribute.*

Tabel 3. Hasil Pengujian ABAC LPBD

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**	***Permit***
	Create Cabinte	*Create*		***Permit***
	Create Rack	*Create*		***Permit***
	Create Bag	*Create*		***Permit***
	Input Data Case COC	*Input*		***Permit***
Investigator	*Download Digital Evidence*	*Download*	*IP Address:* **192.168.0.108** *Mac Address:* **e4:ce:8f:19:c7:7a** *Time Access:* **24**	***Permit***
	Complete Digital Evidence	*Complete*		***Permit***
Officer	*Delete Digital Evidence*	*Delete*	*IP Address:* **192.168.1.1** *Mac Address:* **Fe80::4c2c:f62a:de:a57c%11** *Time Access:* **24**	***Permit***
	Change Password	*Change*		***Permit***
	Validate Digital Evidence	*Validate*		***Permit***
	Validate Case Status	*Validate*		***Permit***
	Validate Data COC	*Validate*		***Permit***
	Download Form COC	*Download*		***Permit***
Subject	*Resource*	*Actions*	*Environment*	*Output*
	Change Code Signature	*Change*		***Permit***
Lawyer	*Download Form COC*	*Download*	*IP Address:* **192.168.0.106** *Mac Address:* **d5:6d:7e:19:c2:9c** *Time Access:* **09.00-15.00**	***Permit***

Tabel 3 menjelaskan bahwa hasil pengujian *access control* LPBD meliputi semua komponen yang digunakan sebagai *attribute* dalam rancangan XACML *policy* berupa *attribute subject, resource, actions,* dan *environment* menghasilkan *output* pengujian sebanyak 15 *permit* yang artinya semua *attribute* yang digunakan dapat berjalan dengan baik dan berfungsi sebagaimana mestinya.

Pada bagian ini juga akan dijelaskan bahwa model *access control* yang paling memungkinkan digunakan pada LPBD yaitu ABAC karena dengan pertimbangan bahwa pendekatan menggunakan ABAC lebih fleksibel. Sebagaimana yang disebutkan oleh [17] bahwa ABAC akan lebih banyak digunakan dalam hal fleksibilitas dalam penerapat *attribute* terhadap *user*, dalam penelitian lain yang dikukan oleh [18] juga menyebutkan bahwa ABAC memiliki sejumlah *feature* yang lebih baik dari model pada generasi sebelumnya, salah satu diantara *feature* tersebut adalah bahwa ABAC memungkinkan pemberian *grant access control* melalui kombinasi dari sejumlah *attribute* elemen autorisasasi seperti: *subject*, *resource*, *actions*, dan *environment* menjadi satu keputusan *access control*.

Berdasarkan permasalahan yang terdapat pada latar belakang penelitian ini, bahwa terdapat permasalahan pada *access control* LPBD sebelumnya, yang dibuat hanya dengan mekanisme authentikasi dan otorisasi *user* saja yaitu metode authentikasi dan otorisasi *username* dan *password*, tidak adanya parameter lain yang mendukung proses otentifikasi dan otorisasi yang lebih kompleks. Model *attribute based access control* (ABAC) yang usulkan pada LPBD saat ini, merupakan sebuah solusi model akses kontrol yang lebih baik dan 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 [17] Hal ini telah sesuai dengan apa yang dikerjakan saat ini, bahwa model *attribute based access control* (ABAC) yang rancang khusus untuk LPBD telah menerapkan aturan *policy* berupa *attribute subject, resource, action* dan *environment.* Hal ini karena sebuah *request* akses tidak hanya memenuhi otentifikasi *user* saja, akan tetapi wajib memenuhi *rule policy* yang telah diberikan sebagai otorisasi terhadap *object* yang ada. Dengan adanya rancangan ABAC pada LPBD ini juga dapat meningkatkan tingkat keamanan sistem LPBD yang berisi bukti digital yang harus tetap terjaga keasliannya.

VI. PENUTUP

Berdasarkan penjelasan rancangan konsep model *attribute based access control* (ABAC) pada lemari penyimpanan bukti digital (LPBD) yang telah dijelaskan sebelumnya maka dapat disimpulkan bahwa perancangan ABAC pada LPBD ini diawali dengan melakukan perancangan model ABAC LPBD, dilanjutkan dengan membuat konsep XACML *policy* dalam bentuk *policy statement* untuk dapat menyesuaikan antara kebutuhan ABAC dan kebutuhan LPBD, serta diimplementasikan dalam bentuk halaman *login*. Dengan hasil pengujian *access control* yang berjalan dengan baik dan berfungsi sebagaimana mestinya.

Selain itu pendekatan menggunakan metode ABAC ini telah mampu menjadi solusi atas permasalahan *access control* LPBD sebelumnya. Metode ini juga dapat menjadi solusi dalam meningkatkan tingkat keamanan sistem LPBD yang dimana berisi bukti digital yang harus tetap terjaga keasliannya. Penelitian selanjutnya dapat memperbaiki akses kontrol yang kini belum dapat dilengkapi dengan uji coba *schema* rancangan XACML. Untuk itu perlu dilakukan penelitian berkaitan dengan *schema* struktur XACML yang ada. Selain melakukan pengujian *schema* struktur XACML perlu juga melakukan validasi terhadap rancangan XACML yang telah dibuat.

DAFTAR PUSTAKA

[1] Y. Prayudi, "Problema dan Solusi Digatal Chain of Custody Yudi Prayudi Abstract," *Semin. Nas. Sains dan Teknol. Informas*, no. 2011, 2014.

[2] Y. Prayudi and T. K. Priyambodo, "Secure and Trusted Environment as a Strategy to Maintain the Integrity and Authenticity of Digital Evidence," pp. 299–314, 2015.

[3] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of Smartphones Using Soft System Methodology," *Int. J. Electr. Comput. Eng.*, vol. 7, no. 5, p. 2806, 2017.

[4] I. Riadi, Sunardi;, and A. Firdonsyah, "Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework," *Int. J. Cyber-Security Digit. Forensics*, vol. 16, no. 4, pp. 198–205, 2017.

[5] Y. Prayudi and A. Ashari, "Digital Evidence Cabinets : A Proposed Framework for Handling Digital Chain of Custody," no. 9, pp. 30–36, 2014.

[6] K. Widatama, "Konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML," *Semin. Nas. Inform. dan Apl. ke-3 dengan tema "Digital Evid. Comput. Crime,"* p. 23, 2017.

[7] Y. A. Younis, K. Kifayat, M. Merabti, and Dummy, "An access control model for cloud computing environments," *Proc.-2nd Int. Conf. Adv. Comput. Netw. Secur. ADCONS 2013*, vol. 19, no. 1, pp. 226–231, 2013.

[8] W. Stallings and L. Brown, *Computer Security : Principles and Practice*, 3rd Editio. USA: Pearson Education International, 2015.

[9] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "Digital Evidence Cabinets : A Proposed Frameworks for Handling Digital Chain of Custody," *Int. J. Comput. Appl.*, vol. 109, no. 9, pp. 30–36, 2014.

[10] N. Widiyasono, I. Riadi, and A. Luthfi, "Investigation on the services of private cloud computing by using ADAM Method," *Int. J. Electr. Comput. Eng.*, vol. 6, no. 5, pp. 2387–2395, 2016.

[11] A. Kurniawan, I. Riadi, and A. Luthfi, "Forensic analysis and prevent of cross site scripting in single victim attack using open web application security project (OWASP) framework," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 6, pp. 1363–1371, 2017.

[12] T. Priebe, W. Dobmeier, C. Schläger, and N. Kamprath, "Supporting attribute-based access control in authorization and authentication infrastructures with ontologies," *J. Softw.*, vol. 2, no. 1, pp. 27–38, 2007.

[13] R. Sandhu, "Security Models : Past , Present and Future," no. August. Institute for Cyber Security, UTSA USA, San Antonio, TX, USA, pp. 1–28, 2010.

[14] N. Dan and C. Yuan, "Attribute Based Access Control (ABAC) -based cross-domain access control in service-oriented architecture (SOA)," pp. 1405–1408, 2012.

[15] X. Son Ha, T. Luong Khiem, and T. K. Dang, "Rew – XAC : An approach to rewriting request for elastic ABAC enforcement with dynamic policies," *Int. Conf. Advenced Comput. Appl.*, pp. 25–31, 2016.

[16] A. A. Abd El-Aziz and A. Kannan, "A comprehensive presentation to XACML," *Third Int. Conf. Comput. Intell. Inf. Technol. (CIIT 2013)*, pp. 155–161, 2013.

[17] V. C. Hu *et al.*, "Guide to attribute based access control (abac) definition and considerations," *NIST Spec. Publ.*, vol. 800, p. 162, 2014