# BAB 1
# Pendahuluan

## 1.1 Latar Belakang

Lemari penyimpanan bukti digital (LPBD) merupakan tempat untuk menyimpan file bukti digital. Bukti digital bersifat rentan mengalami kerusakan dan dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Bukti digital yang mengalami kerusakan tidak dapat diakui di dalam proses peradilan. *User* yang mengakses LPBD juga harus dibedakan antara *user* yang satu dengan user yang lain. Sebagai contoh, yang boleh mengunduh file bukti digital hanyalah *examiner* atau *external* jika diperlukan. Karena *examiner* merupakan orang yang bertugas untuk mengolah bukti digital tersebut dalam suatu kasus. *External* juga diperbolehkan untuk mengunduh file bukti digital tersebut apabila mendapat persetujuan dari peradilan. Pihak *external* yang dimaksud disini yaitu kuasa hukum terdakwa (*lawyer*) dan *external examiner* yang juga ditugaskan untuk mengolah file bukti digital tersebut. Selain *examiner* dan *external* tidak diperbolehkan mengunduh file bukti digital.

Bukti digital sangat rentan terhadap kerusakan oleh sebab itu dalam membuat LPBD diperlukan kemanan khusus agar file bukti digital yang terdapat didalamnya akan terjamin keamanannya. Redfield & Date (2014) melakukan penelitian tentang proses perekaman dan penyimpanan bukti digital. Mereka memperkenalkan skema Gringotts sebuah sistem untuk menjaga integritas pada proses perekaman, transfer dan penyimpanan data dengan bantuan *digital signatures* sebagai keamanan data dari file bukti digital tersebut. Dengan bantuan *digital signature* maka file bukti digital tersebut terjamin keasliannya dan dapat dipertanggungjawabkan di depan peradilan.

Bukti digital tidak boleh diakses oleh sembarang *user* maka di dalam LPBD perlu ditambahkan dengan adanya *access control*. *Access control* ini berfungsi untuk mengontrol siapa saja yang mempunyai hak untuk mengakses file di dalamnya. Sehingga file bukti digital dapat diakses oleh *user* yang sesuai dengan hak aksesnya tersebut dan terjamin keamanannya.

*Access control* sendiri memiliki beberapa model salah satunya yaitu ABAC. ABAC merupakan salah satu model dari *access control* yang baru. Mengingat ABAC memiliki fungsi yang fleksibel, tidak salah jika ABAC ini akan digunakan sebagai model *access*

*control* yang banyak dipakai dalam sistem keamanan saat ini dan untuk tahun-tahun yang akan datang.

Model ABAC ini mempunyai fungsi yang fleksibel sehingga memungkinkan bersinggungan dengan banyak sekali atribut, hal ini akan menjadi sangat kompleks dan dapat menimbulkan munculnya *inconsistency* dan *incompleteness.* Ini memungkinkan terjadinya *user* yang seharusnya memiliki hak akses *permit* dapat berubah menjadi *deny* begitu juga sebaliknya. Dikhawatirkan terdapat *user* yang tidak memiliki hak akses *permit* dapat mengakses yang bukan menjadi haknya dan *user* yang memiliki hak akses *permit* tidak bisa mengaksesnya. Oleh karena itu implementasi dari ABAC ini harus didukung oleh kebijakan policy yang tepat dan tervalidasi dengan baik agar keamanan dalam LPBD berjalan dengan baik dan terhindar dari *inconsistency* dan *incompleteness*. Untuk mengatasi *inconsistency* dan *incompleteness* menurut Mankai & Logripppo (2005) yaitu dilakukan dengan cara kombinasi algoritma.

Model validasi dari ABAC ada beberapa macam, salah satu contoh model yang baik yaitu model checking. Karena model ini akan menguji bagian-bagian dari sistem sehingga sistem tersebut dapat diketahui jika terdapat *error.* Menurut Aqib & Shaikh (2015) model checking ini menggunakan linear temporal logic (LTL) untuk menggambarkan model checker SPIN yang digunakan untuk verifikasi dan validasi *policy.* SPIN merupakan metode pengecekan yang dilakukan dengan perulangan sedangkan LTL sendiri memiliki fungsi yaitu akan bernilai benar *(true)* atau salah *(false)* berdasarkan input yang telah ditetapkan sebelumnya. Sehingga menurut penulis metode ini cocok digunakan untuk validasi Policy Statement dalam LPBD.

*Tool* untuk melakukan validasi ada beberapa macam jenisnya. Salah satu contoh tool yang baik yaitu *Access Control Policy Testing* atau yang dikenal ACPT (Hwang, Xie, Hu, & Altunay, 2010). Selain lengkap, ACPT banyak digunakan untuk validasi ABAC penelitian yang telah dilakukan sebelumnya. Di dalam ACPT terdapat beberapa kombinasi algoritma yang digunakan untuk menguji policy statement tersebut.

## 1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini yaitu:

1. Bagaimana membangun *policy statement* berbasiskan pada ABAC pada LPBD
2. Bagaimana menguji *policy statement* tersebut dengan menggunakan beberapa algoritma untuk mengetahui terjadinya *inconsistency* & *incompleteness* atau tidak
3. Bagaimana memastikan *user* dalam LPBD mendapatkan hak akses sesuai dengan tugasnya masing-masing

## 1.3 Batasan Masalah

Batasan masalah dalam penelitian ini yaitu:

1. *Policy statement* yang diuji mengambil contoh *policy statement* di dalam LPBD. (Fadli, 2018)
2. *Tool* yang dipakai dalam penelitian ini yaitu ACPT

## 1.4 Tujuan Penilitian

1. Membangun *policy statement* yang benar pada LPBD
2. Menguji validasi policy statement tersebut untuk mengetahui terjadinya *inconsistency* dan *incompleteness* atau tidak.
3. Memastikan *user* dalam LPBD mendapatkan hak akses sesuai dengan rule nya

## 1.5 Literatur Review

Literatur review dalam penelitian ini dapat dilihat pada tabel 1.1

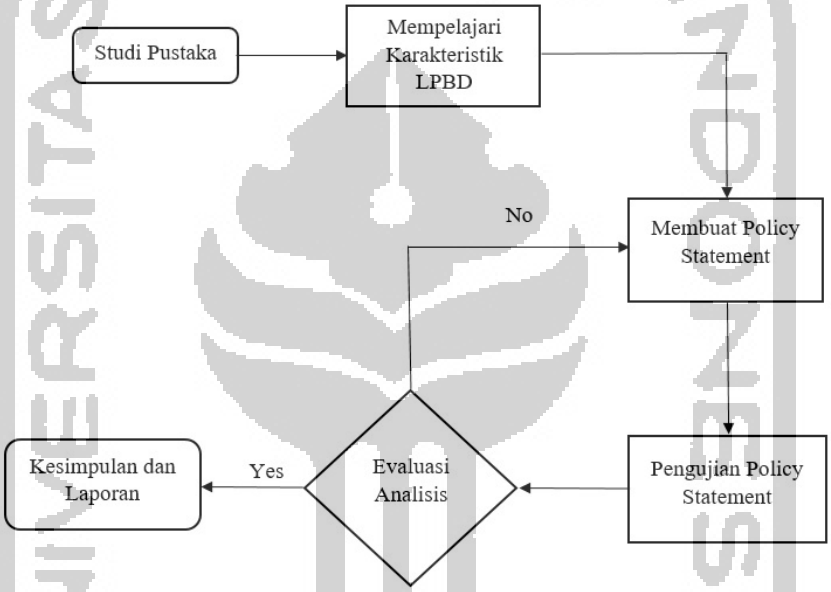
Tabel 1.1 Literatur Review

| **Paper Utama** | **Penerapan** | **Metode Validasi yang digunakan** | **Data yang digunakan** | **Tool** |
|---|---|---|---|---|
| Dianxiang Xu, Yunpeng Zhang (2014) | Konten dalam aplikasi | *Model checking* | *Policy* | ACPT |
| Ang Li, Qinghua Li, Vincent C Hu, Jia Di (2015) | Sistem Database | *Model Checking* | *Policy* | ACPT |
| Nariman Ammar, Zaki Malik, Abdelmounaam Rezgui, Elisa Bertino (2016) | Data Repository | *Dinamic privacy management* | *Policy* | SunXACML |
| Nuo Li, JeeHyun Hwang, Tao Xie (2008) | Aplikasi web | - | *Policy* | SunXACML |
| Muhammad Aqib, Riaz Ahmed Shaikh (2015) | - | *Formal methods, Modal checking methods, matrix based approaches, mining technique, mutation testing technique, others* | *Policy* | - |
| Catherine MS Redfield, Hiroyuki Date (2014) | Penyimpanan Bukti Digital | Skema Gringgot | Bukti Digital | - |
| M Fadly Panende, Imam Riadi, Yudi Prayudi (2017) | LPBD | - | *Policy* | UMU |
| **Usulan Penelitian** | | | | |
| Solusi yang diusulkan | LPBD | *Model Checking* | *Policy statement* | ACPT |

Berdasarkan pada literatur review yang telah dilakukan oleh peneliti-peneliti sebelumnya penulis melakukan penelitian yaitu menguji *policy statement* pada LPBD dengan *model checking*. Proses pengujian *policy statement* tersebut menggunakan *tool* ACPT. Karena ACPT memiliki fitur-fitur untuk membuat dan menguji *policy statement* dengan berbagai macam kombinasi algoritma yang ada. Dalam penelitian ini penulis menggunakan 3 kombinasi algoritma yang terdapat pada ACPT yaitu kombinasi algoritma *first applicable, deny overrides,* dan *permit overrides*.

## 1.6 Metodologi Penelitian

Alur metodologi dalam penelitian ini yaitu seperti pada gambar 1.1




Gambar 1.1 Metodologi Penelitian

1. Studi Pustaka

   Pada tahap ini penulis mencari berbagai sumber referensi dari penelitian-penelitian yang telah dilakukan sebelumnya.

2. Mempelajari Karakteristik LPBD

   Merupakan tahap mempelajari karakteristik-karakteristik yang ada dalam LPBD.

3. Membuat *Policy Statement* LPBD

   Tahap ini membuat *policy statement* untuk LPBD.

4. Pengujian *Policy Statement*

   Tahap ini melakukan pengujian terhadap *policy statement* tersebut menggunakan beberapa kombinasi algoritma yang disediakan oleh ACPT.

5. Evaluasi Analisis

Tahap ini membandingkan hasil dari beberapa pengujian dengan kombinasi algoritma yang berbeda apakah menemukan *inconsistency & incompleteness* atau tidak dan memastikan *user* yang mengakses LPBD berjalan sesuai dengan hak aksesnya.

6. Kesimpulan dan Laporan

   Tahap ini merupakan tahap akhir yaitu menuliskan kesimpulan dan laporan hasil penelitian yang telah dilakukan.

## 1.7 Sistematika Penulisan

Untuk mempermudah penulisan dalam penelitian ini maka dilakukan sistematika penulisan sebagai dasar pembuatan laporan. Sistematika penulisan dalam penelitian ini yaitu:

BAB 1 Pendahuluan

Pada bab ini menjelaskan tentang latar belakang dari permasalahan-permasalahan yang muncul dan akan dicari solusinya dalam penelitian ini.

BAB 2 Tinjauan Pustaka

Bab ini menjelaskan tentang teori-teori yang digunakan untuk menyelesaikan permasalahan yang timbul dalam bab 1. Teori-teori yang dijelaskan pada bagian ini merupakan teori-teori yang berhubungan dengan *access control* dan validasinya.

BAB 3 Metodologi Penelitian

Pada bab ini menggambarkan langkah-langkah yang diambil dalam penelitian ini.

BAB 4 Hasil dan Pembahasan

Hasil penelitian yang dilakukan akan dibahas pada bab ini.

BAB 5 Kesimpulan dan Saran

Pada bab ini menceritakan kesimpulan yang dapat diambil dalam penelitian ini dan saran-saran sebagai bahan masukan untuk mengembangkan dan melanjutkan penelitian ini.