Validasi Policy Statement pada Lemari Penyimpanan Bukti Digital (LPBD)

Achmad Syauqi[1], Imam Riadi[2], Yudi Prayudi[3]
[1,3]Program Studi Teknik Informatika Universitas Islam Indonesia
Jalan Kaliurang Km 14,5 Sleman, Yogyakarta, +62274898444
[2]Program Studi Sistem Informasi Universitas Ahmad Dahlan
Jalan Prof. Dr. Soepomo, S.H Janturan, Yogyakarta, +62274563515
e-mail: **[1]15917101@students.uii.ac.id**, [2]imam.riadi@is.uad.ac.id, [3]prayudi@uii.ac.id

Abstrak

Bukti digital sangat rentan terhadap kerusakan. Oleh sebab itu dalam membuat lemari penyimpanan bukti digital (LPBD) diperlukan adanya access control. Access control sendiri memiliki beberapa model, salah satunya yaitu ABAC. ABAC merupakan salah satu model dari access control yang baru. Karena model ABAC ini mempunyai fungsi yang fleksibel, memungkinkan bersinggungan dengan banyak sekali atribut, hal ini akan menjadi sangat kompleks dan dapat menimbulkan munculnya incosistency dan incompleteness. Maka dari itu implementasi dari ABAC ini harus didukung oleh kebijakan policy yang tepat dan tervalidasi dengan baik agar keamanan dalam LPBD lebih terjamin. Salah satu model pengujian access control yaitu model checking. Model checking ini bersifat memeriksa elemen-elemen di dalam sistem sehingga jika terdapat error maka akan diketahui. Sedangkan tools untuk validasi policy statement terdapat beraneka ragam salah satunya ACPT (Acess Control Policy Testing). Di dalam ACPT terdapat berbagai metode untuk membuat dan menguji policy statement. Pengujian ini dilakukan menggunakan kombinasi algoritma permit overrides dan dilakukan sebanyak 30 kali pengujian. Penelitian ini telah berhasil menguji dan membuktikan bahwa policy statement tersebut tidak menemukan incosistency dan incompleteness. Dalam 30 kali pengujian, policy statement tersebut berjalan sesuai dengan rule yang ada.
Kata kunci: *validasi, policy statement, ABAC, bukti digital*

Abstract

Digital evidence is very vulnerable to damage. Therefore to making digital evidence storage need access control. Access control has several models, one of them is ABAC (Attribute Base Access Control). ABAC is new access control model. ABAC model has a flexible function, allows intersect with many attributes. This will be very complex and causing inconsistency and incompleteness. The implementation of ABAC must be supported by appropriate policies and validated properly in order to the security in DESC runs well. One testing model is model checking. This model while discussing the elements in the system in order to the errors can be identified easily. There are many tools for validating policy statements, one of them is Access Control Policy Testing (ACPT). In ACPT there are various methods for creating and testing policy statements. This test was carried out using a combination of the permit overrides algorithm and carried out as many as 30 tests. This research has succeeded in testing and proving that the policy statement does not find incisistency and incompleteness. In 30 tests, the policy statement goes according to the existing rules.

1. Pendahuluan

Bukti digital sangat rentan terhadap kerusakan. Oleh sebab itu dalam membuat lemari penyimpanan bukti digital (LPBD) diperlukan kemanan khusus agar file bukti digital yang terdapat didalamnya akan terjamin keamanannya.[1] Redfield & Date pernah 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.

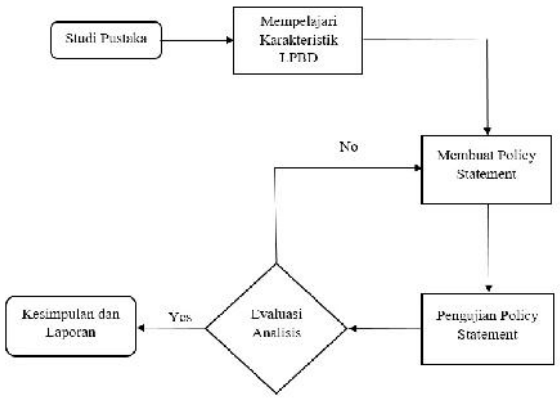
Bukti digital tidak boleh diakses oleh sembarang *user*. Maka di dalam LPBD perlu ditambahkan dengan adanya *access control. Access control* sendiri memiliki beberapa model salah satunya yaitu ABAC [2] [3]. ABAC merupakan salah satu model dari *access control* yang baru. ABAC memiliki fungsi yang fleksibel sehingga ABAC digunakan sebagai model *access control* yang banyak dipakai dalam sistem keamanan saat ini dan untuk tahun-tahun yang akan datang [4] [5].

Model ABAC ini mempunyai fungsi yang fleksibel sehingga memungkinkan bersinggungan dengan banyak sekali atribut. Ini akan menjadi sangat kompleks dan dapat menimbulkan munculnya *incosistency* dan *incompleteness*. Sehingga memungkinkan terjadinya *user* yang seharusnya memiliki hak akses *permit* dapat berubah menjadi *deny*. Begitu juga sebaliknya. Oleh karena itu implementasi dari ABAC ini harus didukung oleh kebijakan policy yang tepat dan tervalidasi dengan baik.

Model validasi dari ABAC ada beberapa macam [6]. 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*. Sedangkan *tools* untuk melakukan validasi ada beberapa macam jenisnya. Salah satu contoh tools yang baik yaitu *Access Control Policy Testing* atau yang dikenal ACPT [7] [8]. Di dalam ACPT terdapat beberapa kombinasi algoritma yang digunakan untuk menguji *policy statement* tersebut.

2. Metode Penelitian

Alur dalam penelitian ini dapat dilihat pada gambar 1:



Gambar 1. Metode Penelitian

1. Policy Statement
   Policy statement dalam penelitian ini mengambil contoh policy statement dalam LPBD [9]
2. *Software*
   Software yang digunakan untuk melakukan pengujian policy statement adalah ACPT (Access Control Policy Testing)

3. Model
   Model yang digunakan untuk penelitian ini yaitu model checking dengan salah satu kombinasi algoritma yang disediakan oleh ACPT yaitu *permit overrides*.

2.1. Literatur Review

Literatur review dalam penelitian ini dapat dilihat pada tabel 1:

Tabel 1. Literatur Review

Paper Utama	Aplikasi	Validasi	Data yang digunakan	Tools
Catherine MS Redfield, Hiroyuki Date (2014) [1]	Digital evidence storage	Skema Gringgot	Bukti Digital	-
Dianxiang Xu, Yunpeng Zhang (2014) [3]	Application content	Model checking	Policy	ACPT
Ang Li, Qinghua Li, Vincent C Hu, Jia Di (2015) [8]	Database system	Model Checking	Policy	ACPT
Nariman Ammar, Zaki Malik, Abdelmounaam Rezgui, Elisa Bertino (2016) [7]	Data Repository	Dinamic privacy management	Policy	SunXACML
Nuo Li, JeeHyun Hwang, Tao Xie (2008) [10]	Web application	-	Policy	SunXACML
Muhammad Aqib, Riaz Ahmed Shaikh (2015) [6]	-	Formal methods, Model checking methods, matrix based approaches, mining technique, mutation testing technique, others	Policy	-
M Fadly Panende, Imam Riadi, Yudi Prayudi (2018) [9]	Lemari penyimpanan bukti digital	-	Policy	UMU
		Penelitian		
Penelitian	Lemari penyimpanan bukti digital	Model Checking	Policy statement	ACPT

3. Hasil dan Pembahasan

a. Policy Statement LPBD

Policy statement ini mengambil contoh dari *policy statement* dalam LPBD [9] yaitu :

1. *First Responder*
   First Responder mempunyai tugas mengolah TKP untuk menemukan barang bukti elektronik. Kemudian mengakuisisi barang bukti elektronik tersebut sehingga mendapatkan bukti digital dan mengunggahnya ke dalam LPBD. Sehingga di dalam LPBD mempunyai hak akses *permit* yaitu *upload digital evidence, create cabinet, create rack, create bag, input data evidence.* Selain hak akses yang diberikan tersebut *First Responder* tidak diijinkan mengaksesnya atau *deny.*
2. *Examiner*
   Examiner mempunyai tugas mengolah barang bukti digital utnuk mendapatkan bukti digital sesuai dengan kasusnya. Sehingga dalam LPBD mempunyai hak akses *permit* yaitu *download digital evidence, input data case.* Selain hak akses yang diberikan tersebut *examiner* tidak diijinkan mengaksesnya atau *deny.*
3. *Officer*
   Officer mempunyai tugas mengatur segala sesuatu dalam LPBD sehingga mempunyai hak akses *permit* yaitu *create username, create password, create signature, delete digital evidence, validate digital evidence, validate data evidence, validate data case, create form COC, download form COC.* Selain hak akses yang diberikan tersebut *Officer* tidak diijinkan mengaksesnya atau *deny.*
4. *External*
   External merupakan pihak diluar praktisi resmi. Yang termasuk *external* dalam LPBD yaitu *lawyer* dan *external examiner*. *External* diberikan hak akses permit yaitu *download digital evidence* dan *download form COC*. Selain hak akses tersebut *external* tidak diijinkan mengaksesnya atau *deny.*

Sedangkan rule yang dibuat untuk LPBD dapat dilihat pada tabel 2:

Tabel 2. Rule dalam LPBD

Subject	Resource	Action	Environment	Decision
First Responder	Digital Evidence	Upload	Time	Permit
			Ip Address	
			Mac Address	
	Cabinet	Create	Time	Permit
			Ip Address	
			Mac Address	
	Rack	Create	Time	Permit
			Ip Address	
			Mac Address	

	Bag	Create	Time	Permit
			Ip Address	
			Mac Address	
	Data Evidence	Input	Time	Permit
			Ip Address	
			Mac Address	
Examiner	Digital Evidence	Download	Time	Permit
			Ip Address	
			Mac Address	
	Data Case	Input	Time	Permit
			Ip Address	
			Mac Address	
Officer	Username	Create	Time	Permit
			Ip Address	
			Mac Address	
	Password	Create	Time	Permit
			Ip Address	
			Mac Address	
	Signature	Create	Time	Permit
			Ip Address	
			Mac Address	
	Digital Evidence	Delete	Time	Permit
			Ip Address	
			Mac Address	
	Digital Evidence	Validate	Time	Permit
			Ip Address	
			Mac Address	

	Data Evidence	Validate	Time	Permit
			Ip Address	
			Mac Address	
	Data Case	Validate	Time	Permit
			Ip Address	
			Mac Address	
	Form COC	Create	Time	Permit
			Ip Address	
			Mac Address	
	Form COC	Download	Time	Permit
			Ip Address	
			Mac Address	
External	Form COC	Download	Time	Permit
			Ip Address	
			Mac Address	
	Digital Evidence	Download	Time	Permit
			Ip Address	
			Mac Address	

Berdasarkan pada rule LPBD diatas kemudian diterapkan ke dalam ACPT:

1. *Subject*
   Di dalam *attribute subject* berisi *attribute value : first responder, examiner, officer,* dan *external.*
2. *Resource*
   Di dalam *attribute resource* berisi *attribute value*: *Digital_Evidence, Cabinet, Rack, Bag, Data_Evidence, Data_Case, Username, Password, Signature, FormCOC.*
3. *Action*
   Di dalam *attribute action* berisi *attribute value*: *create, upload, input, download, delete, validate*
4. *Environment*
   Di dalam *attribute environment* berisi *attribute value*: *Fulfilled, Not Fulfilled* yang mewakili dari *attribute value : Time, Ip_Address & Mac_Address.*

b. Pengujian *Policy Statement*

Pengujian *policy statement* menggunakan salah satu kombinasi algoritma yang telah telah disediakan oleh ACPT yaitu *permit overrides. Permit overrides* yaitu kombinasi algoritma

yang menggabungkan keputusan sedemikian rupa sehingga jika terdapat keputusan yang *permit*. Maka keputusan itu yang akan menang. Pengujian menggunakan kombinasi algoritma *permit overrides* dilakukan sebanyak 30 kali pengujian karena dalam statistik angka 30 adalah *sample* minimal untuk populasi yang besar. Hal ini dilakukan agar *policy statement* tersebut benar-benar teruji dan terhindar dari *inconsistency* dan *incompleteness.* Dalam 1 kali melakukan pengujian menggunakan ACPT menghasilkan 60 kombinasi policy statement yang beraneka ragam. Hasil pengujian dapat dilihat pada tabel 3:

Tabel 3. Hasil Pengujian

Pengujian Ke	Hasil Pengujian	
	Decision Permit	Decision Deny
1	3	57
2	2	58
3	1	59
4	2	58
5	2	58
6	3	57
7	3	57
8	3	57
9	3	57
10	2	58
11	1	59
12	1	59
13	4	56
14	3	57
15	2	58
16	1	59
17	2	58
18	1	59
19	2	58
20	2	58
21	4	56
22	1	59
23	2	58
24	1	59
25	3	57
26	1	59
27	1	59
28	5	55
29	1	59
30	2	58

Hasil pengujian yang menghasilkan *decision permit* sesuai dengan rule LPBD dapat dilihat pada tabel 4:

Tabel 4. *Decision Permit* Kombinasi Algoritma *Permit Overrides*

Subject	Resource	Action	Environment	Decision	Pengujian Ke
First Responder	Digital Evidence	Upload	Fulfilled	Permit	
	Cabinet	Create	Fulfilled	Permit	
	Rack	Create	Fulfilled	Permit	
	Bag	Create	Fulfilled	Permit	
	Data Evidence	Input	Fulfilled	Permit	
Examiner	Digital Evidence	Download	Fulfilled	Permit	
	Data Case	Input	Fulfilled	Permit	1,2,7,9,10,13,14,15, 17,19, 20,21,23,28

Officer	Username	Create	Fulfilled	Permit	
	Password	Create	Fulfilled	Permit	1,2,3,4,5,6,7,8,9,10,11, 12,13,14,15,16,17,18, 19,20,21,22,23,24,25, 26,27,28, 29,30
	Signature	Create	Fulfilled	Permit	
	Digital Evidence	Delete	Fulfilled	Permit	
	Digital Evidence	Validate	Fulfilled	Permit	
	Data Evidence	Validate	Fulfilled	Permit	6,8,25,28
	Data Case	Validate	Fulfilled	Permit	13,21,28
	Form COC	Create	Fulfilled	Permit	
	Form COC	Download	Fulfilled	Permit	1,4,5,6,7,8,9,13,14, 21,25,28,30
External	Form COC	Download	Fulfilled	Permit	
	Digital Evidence	Download	Fulfilled	Permit	

Sedangkan hasil pengujian dengan *decision deny* pada kombinasi *first applicable* terdapat bermacam-macam kombinasinya. Sampel dari hasil pengujiannya dapat dilihat pada tabel 5:

Tabel 4. *Decision Deny* Kombinasi Algoritma *Permit Overrides*

Subject	Reasource	Action	Environment	Decision
First Responder	Form COC	Validate	Fulfilled	Deny
	Signature	Download	Fulfilled	Deny
	Password	Delete	Fulfilled	Deny
	Username	Input	Fulfilled	Deny
	Data Case	Delete	Not Fulfilled	Deny
Examiner	Cabinet	Input	Not Fulfilled	Deny
	Digital Evidence	Delete	Fulfilled	Deny
Officer	Digital Evidence	Input	Not Fulfilled	Deny
	Cabinet	Upload	Fulfilled	Deny
	Rack	Download	Fulfilled	Deny
	Bag	Create	Fulfilled	Deny
	Data Evidence	Input	Fulfilled	Deny
	Data Case	Download	Not Fulfilled	Deny
External	Digital Evidence	Validate	Not Fulfilled	Deny
	Cabinet	Download	Fulfilled	Deny

4. Kesimpulan

Pengujian *policy statement* dalam LPBD merupakan kewajiban sebelum diterapkan ke dalam sistem. Berdasarkan hasil pengujian telah menghasilkan kesimpulan bahwa policy statement tersebut berjalan sesuai dengan rule yang ada. User yang mempunyai hak akses permit setelah pengujian tetap mempunyai hak akses permit dan sebaliknya. Selama melakukan pengujian dalam penelitian ini tidak menemukan *incosistency* dan *incompleteness*. Penulis berharap penelitian ini dilanjutkan dengan metode serta *tools* lain sehingga validasi menjadi lebih valid.

Daftar Pustaka

[1] C. M. S. Redfield and H. Date, "Gringotts: Securing data for digital evidence," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2014-January, pp. 10–17, 2014.

[2] K. D. Forensik, P. Studi, M. Teknik, P. Pascasarjana, F. Teknologi, and U. I. Indonesia, "Eksplorasi ABAC dan XACML untuk Design Access Control pada Resource Digital Fauzan Natsir," 2019.

[3] D. Xu and Y. Zhang, "Specification and analysis of attribute-based access control policies: An overview," *Proc. - 8th Int. Conf. Softw. Secur. Reliab. - Companion, SERE-C 2014*, pp. 41–49, 2014.

[4] A. Cavoukian, M. Chibba, G. Williamson, and A. Ferguson, "The Importance of ABAC : Attribute-Based Access Control to Big Data : Privacy and Context," 2015.

[5] L. Krautsevich and A. Lazouski, "Towards Policy Engineering for Attribute-Based," no. 256980, pp. 85–102, 2013.

[6] M. Aqib and R. Ahmed Shaikh, "Analysis and Comparison of Access Control Policies Validation Mechanisms," *Int. J. Comput. Netw. Inf. Secur.*, vol. 7, no. 1, pp. 54–69, 2015.

[7] N. Ammar, Z. Malik, A. Rezgui, and E. Bertino, "XACML policy evaluation with dynamic context handling," *2016 IEEE 32nd Int. Conf. Data Eng. ICDE 2016*, no. Table I, pp. 1570–1571, 2016.

[8] A. Li, Q. Li, V. C. Hu, and J. Di, "Evaluating the capability and performance of access control policy verification tools," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, vol. 2015-December, pp. 366–371, 2015.

[9] M. F. Panende, I. Riadi, and Y. Prayudi, "Konsep Attribute Based Access Control (Abac) Pada Lemari Penyimpanan Bukti Digital (Lpbd)," *J. Tek. Inform.*, vol. 11, no. 1, pp. 85–94, 2018.

[10] N. Li, J. Hwang, and T. Xie, "Multiple-implementation testing for XACML implementations," pp. 27–33, 2008.