IMPLEMENTASI KONTROL AKSES PADA WEB BERBASIS BLOCKCHAIN

Proposal Tugas Akhir

Kelas MK Penulisan Proposal (CCH4A3)

1301174078

MUHAMMAD RIFKI FAUZAN

Program Studi Sarjana S1 Informatika

Fakultas Informatika

Universitas Telkom

Bandung

2020

Lembar Persetujuan

IMPLEMENTASI KONTROL AKSES PADA WEB BERBASIS BLOCKCHAIN

IMPLEMENTATION OF ACCESS CONTROL ON BLOCKCHAIN-BASED WEB

NIM :1301174078

Muhammad Rifki Fauzan

Proposal ini diajukan sebagai usulan pembuatan tugas akhir pada
Program Studi Sarjana S1 Informatika
Fakultas Informatika Universitas Telkom

Bandung, November 2020
Menyetujui

Calon Pembimbing 1	Calon Pembimbing 2
Parman Sukarno, ST, M.Sc, Ph.D	Aulia Arif Wardana, S.Kom., M.T.
NIP:	NIP:

ABSTRAK

Kontrol merupakan suatu komponen yang sangat krusial dan penting dalam keamanan sistem. Biasa digunakan untuk melindungi suatu data penting atau sebuah tindakan yang sensitif. Salah satunya adalah penggunaan pada *web application.* Pada kontrol akses terdapat dua komponen, yaitu otentikasi dan otorisasi. Otentikasi digunakan untuk metode pengamanan dalam memverifikasi pengguna. Lalu, Otorisasi digunakan untuk mengatur hak akses pada *web application* dengan tujuan membatasi akses penggunanya. Penyimpanan hak akses pada *web* banyak menggunakan *database*. Namun, terdapat sebuah resiko apabila menggunakan penyimpanan pada *database*, yaitu serangan *SQL Injection*. Untuk mengatasi masalah tersebut terdapat teknologi baru, yaitu *blockchain*. Keunggulan dari *blockchain* salah satunya adalah dapat mencegah serangan *SQL Injection*. *Blockchain* tidak menggunakan perintah seperti *SQL* dan menggunakan teknik *hash* untuk keamanan penyimpanan data. Pada penelitian ini penyimpanan hak akses akan digantikan dengan teknologi *blockchain*. Oleh karena itu, pembuatan *web application* yang akan dibangun adalah pengaturan kontrol akses menggunakan *blockchain.*

Kata Kunci: kontrol akses, *blockchain, web application*.

Daftar Isi

1. PENDAHULUAN

1.1. Latar Belakang

Pada era digital saat ini, teknologi informasi berkembang semakin pesat dan sebagian besar sudah mempengaruhi kebutuhan hidup manusia. Salah satunya pada perkembangan *web*. Melalui *web*, semua orang dapat mengakses banyak informasi-informasi yang tersebar luas diinternet [1]. Namun, tidak semua informasi yang ada di *web* dapat diakses oleh semua orang. Ada hal yang dinamakan kontrol akses, yang digunakan untuk mengatur hak akses seseorang untuk dapat mengakses suatu informasi tertentu. Salah satu komponen dari kontrol akses ini adalah otorisasi. Otorisasi merupakan sebuah komponen keamanan yang digunakan untuk melindungi suatu data penting atau sebuah tindakan yang sensitif. Otorisasi dapat digunakan untuk memberikan hak istimewa kepada seseorang, agar dapat mengakses suatu data yang memiliki hak akses terbatas [2].

Otorisasi ini dimaksudkan agar suatu data hanya dapat terlindungi dengan membatasi hak akses. Dalam aplikasi *web*, otorisasi diawali dengan memberikan hak akses bagi *user* sesuai dengan kebutuhan. Pengaturan hak akses biasa digunakan dengan menandai suatu akun *user* dengan menyimpan pemberian kewenangannya (*role*) di *database* [3]. Penggunaan *database* sebagai tempat menyimpan pengaturan hak akses ini masih sering digunakan. Namun, terdapat resiko yang cukup tinggi apabila menggunakan sebuah *database*, salah satunya adalah serangan *SQL Injection.* Serangan *SQL Injection* ini adalah suatu serangan yang memasukan atau menyuntikan perintah *SQL* melalui *input data* yang terdapat pada aplikasi web [4]. Serangan *SQL Injection* dapat melakukan berbagai perintah *SQL* yang memungkinkan penyerang dapat mengambil data-data yang ada pada *database*. Apabila serangan ini dapat dilakukan, tidak hanya dapat mencuri data saja, bahkan penyerang dapat melakukan perubahan sampai penghapusan data [5]. Terdapat sebuah teknologi bernama *blockchain* yang akan menggantikan *database* sebagai tempat menyimpan hak akses tersebut. *Blockchain* memiliki sebuah kelebihan yang dapat menghindari serangan *SQL Injection* [6], hal ini dikarenakan pengunaan *Blockchain* tidak seperti perintah *SQL* dan juga teknik penyimpanan pada *Blockchain* menggunakan teknik *hash* untuk membentuk rantai satu blok dengan blok yang lainnya dimana pada blok tersebut terdapat data yang disimpan [13].

Oleh karena itu, akses kontrol yang dilakukan pada penelitian kali ini adalah dengan menggunakan *blockchain.* Pada penelitian ini, penulis menambahkan suatu fitur keamanan, yaitu pengaturan kontrol akses pada *web* berbasis blockchain. Hal ini dimaksudkan sebagai pengamanan *web* untuk mencegah *user* mengakses halaman yang tidak diizinkan atau hanya dapat melakukan sesuatu pada halaman yang diizinkan saja pada suatu *web*. Harapannya dengan adanya penelitian ini dapat meningkatkan keamanan aplikasi *web*.

1.2. Perumusan Masalah

Berdasarkan pemaparan latar belakang, dibuat perumusan masalah yang akan menjadi acuan untuk penelitian. Permasalahan yang dibahas adalah Bagaimana cara mengimplementasikan kontrol akses menggunakan *blockchain* pada aplikasi *web*.

1.3. Tujuan

Berdasarkan perumusan masalah yang telah ditentukan, maka dibuat juga tujuan dari penelitian ini, yaitu Membangun aplikasi *web* dengan pengaturan kontrol akses berbasis *blockchain*.

1.4. Batasan Masalah

Batasan masalah dari penelitian ini, yaitu aplikasi *web* yang dibuat adalah *web* aplikasi pengamanan ijazah dan transkrip berbasis *blockchain* dan *smart contract.*

1.5. Rencana Kegiatan

Dalam pengerjaan tugas akhir ini, rencana kegiatan yang dilakukan adalah sebagai berikut:

1. Identifikasi Masalah dan Studi Literatur

   Pada tahap ini penulis mencoba untuk menemukan masalah yang berkaitan dengan penerapan *blockchain* pada *web application*, khususnya pada otorisasi hak akses pada *web* dan membaca beberapa literatur terkait.

2. Perancangan Penelitian

   Pada tahap ini akan dilakukan perancangan penelitian yang bertujuan untuk menjabarkan alur penelitian yang akan dilakukan pada tugas akhir ini.

3. Perancangan Sistem

   Pada tahap ini akan dibuat rancangan sistem *web application* sesuai dengan topik yang diangkat.

4. Pelaksanaan Penelitian

   Pada tahap ini akan dilaksanakan penelitian terkait masalah yang diangkat menggunakan sistem yang telah dirancang.

5. Evaluasi Hasil Penelitian

   Pada tahap ini hasil penelitian yang didapat akan dievaluasi berdasarkan tolak ukur yang telah ditetapkan.

6. Penyusunan Dokumen Akhir

   Penyusunan dokumen akhir berisikan tentang hasil penelitian yang telah dilakukan.

1.6. Jadwal Kegiatan

Tugas akhir ini akan dikerjakan sesuai dengan tabel berikut ini:

Tabel 1 Jadwal Kegiatan Pengerjaan Tugas Akhir

Kegiatan	**Bulan Ke-**						
Identifikasi Masalah dan Studi Literatur	1	2	3	4	5	6	7
Perancangan Penelitian							
Perancangan Sistem							
Pelaksanaan Penelitian							
Evaluasi Hasil Penelitian							
Penyusunan Dokumen Akhir							

2. KAJIAN PUSTAKA

2.1. Penelitian Terdahulu

Terdapat beberapa penelitian terdahulu terkait penggunaan otorisasi hak akses pada aplikasi *web* yang dijadikan sebagai acuan dan bahak kajian pada penelitian ini. Penelitian tersebut dipaparkan pada tabel 2.

Tabel 2 Penelitian Terkait Otorisasi Hak Akses Menggunakan *Blockchain*

No.	Penulis	Judul	Metode	Hasil	Kelebihan	Kekurangan
1.	Michael P Andersen, dkk. [2]	Wave: A decentralized authorization system for iot via blockchain smart contracts	Penggunaan *blockchain smart contract* untuk otorisasi pada IoT	Berhasil mengimplementasikan dan membuktikan efektifitas penggunaan *blockchain smart contract* dalam penggunaan *resource* yang tersedia	Kerahasiaan data terjamin	Belum ada penekanan untuk penerapan pada *web application*
2.	Rubiyanto, dkk. [3]	Implementasi Role-Based Access Control (RBAC) Pada Pemanfaatan Data Kependudukan Ditingkat Kabupaten	Menggunakan RBAC untuk pengaturan hak akses dan *database* sebagai media penyimpanan hak akses	Berhasil melakukan pengaturan hak akses menggunakan RBAC pada *web* yang dibangun	Implementasi pengaturan hak akses memiliki komplesitas yang sederhana	Belum menerapkan penggunaan *blockchain* sebagai tempat penyimpanan
3.	Qurotul Aini, dkk. [12]	Pengamanan Pengelolaan Hak Akses Web Berbasis Yii Framework	Menggunakan RBAC untuk pengaturan hak akses dan *database* sebagai media penyimpanan hak akses	Berhasil melakukan pengaturan hak akses menggunakan RBAC pada *web* yang dibangun	Terdapat pengaturan untuk pengecekan *role* pada Yii *framework*	Belum disinggung terkait pencegahan untuk serangan *SQL Injection*

			dengan Yii *framework*	menggunakan Yii *framework*		
4.	Putri, M. C. I, dkk. [14]	Two factor authentication framework based on ethereum blockchain with dApp as token generation system instead of third-party on web application	Menggunakan *ethereum blockchain* sebagai token yang digunakan untuk otentikasi dua faktor pada sistem *third-party* untuk aplikasi *web*	Berhasil membuat sistem otentikasi menggunakan *ethereum blockchain* untuk aplikasi *web*.	*Token* yang dibangun untuk otentikasi di-*hash* terlebih dahulu sehingga kemungkinan terserangnya serangan MITM sulit untuk dilakukan dan juga pengguna tidak perlu memasukan *token* secara manual.	Penerapan keamanan menggunakan *blockchain* pada *web* belum menerapkan kontrol akses sepenuhnya, otorisasi belum diterapkan pada sistem sehingga kelemahan sistem terdapat pada keamanan hak aksesnya.

Pada penelitian diatas telah disimpulkan penelitian-penelitian yang menggunakan pendekatan yang berbeda-beda, akan tetapi maksud dan tujuannya sama, yaitu mengamankan aplikasi *web* dengan mengimplementasikan kontrol akses. Namun, dalam pengimplementasian kontrol akses yang dilakukan masih banyak menggunakan *database* pada umumnya sehingga tebilang cukup rentan. Maka, dilakukan perubahan dalam pengimplementasian kontrol aksesnya, yaitu dengan menggunakan *Blockchain* sebagai media penyimpanannya. Pada tugas akhir ini akan melakukan pengujian terhadap aplikasi *web* yang dibangun yang telah menggunakan kontrol akses menggunakan *blockchain* menggunakan serangan *SQL Injection* agar terlihat apakah sistem yang dibangun dapat menahan serangan tersebut atau tidak. Apabila tahan terhadap serangan *SQL Injection*, maka dapat disimpulkan bahwa pengimplementasian kontrol akses menggunakan *blockchain* aman terhadap serangan *SQL Injection*.

2.2. Dasar Teori

2.2.1. *Blockchain*

Pada dasarnya *blockchain* adalah basis data terdistribusi dari *record* atau *public ledger* dari semua transaksi atau peristiwa digital yang telah dieksekusi dan dibagikan antara pihak yang berpartisipasi. Setiap transaksi yang dilakukan diverifikasi dengan consensus mayoritas oleh partisipan yang ada pada sistem.

Setelah dimasukan ke dalam sistem, data tidak akan pernah bisa dihapus. Transaksi yang dilakukan akan direkam dalam satu buah *block*, dimana setiap *blocki* ini terhubung dengan *block* lain yang ada sebelum atau sesudah sebuah transaksi dilakukan. *Blockchain* berisikan *record* tertentu dan dapat diverifikasi dari setiap transaksi yang pernah dilakukan. *Bitcoin* merupakan mata uang digital *peer-to-peer* terdesentralisasi. *Bitcoin* adalah contoh paling popular yang menggunakan teknologi *blockchain*. Mata uang *Bitcoin* dapat digunakan dalam perdagangan digital yang fungsinya sama dengan mata uang pada dunia nyata [7] [8].

2.2.2. *Ethereum*

Ethereum merupakan sebuah teknologi yang ada pada *blockchain* yang menyediakan sebuah aplikasi *platform* terdesentralisasi untuk operasi *smart contract* [9]. *Ethereum* juga memungkinkan penggunanya untuk membuat aplikasi terdesentralisasi dan *smart contract* sendiri, bahkan dapat membuat aturan semaunya untuk kepemilikan sendiri, format transaksi, dan fungsi-fungsi transisinya [10]. Dalam *platform Ethereum* ini, *Bitcoin* berfungsi sebagai mata uang digital yang dapat digunakan untuk membelanjakan atau mentransfer asset digital pada *platform*.

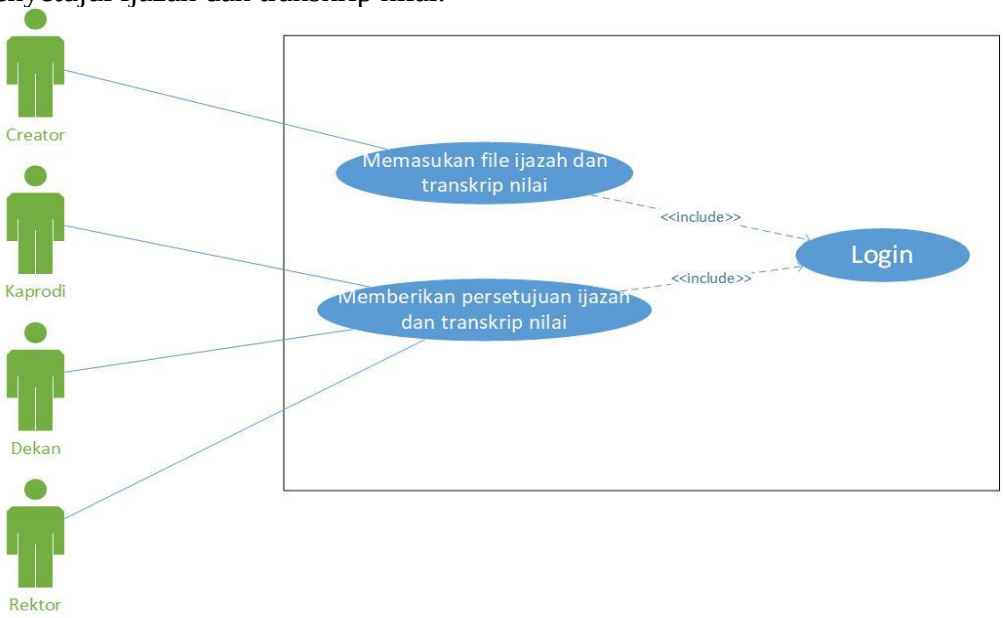
2.2.3. Otorisasi

Otorisasi merupakan sebuah komponen keamanan yang digunakan untuk melindungi suatu data penting atau sebuah tindakan yang sensitif. Otorisasi adalah cara untuk mengatur tingkatan hak akses terhadap suatu data. Otorisasi dapat digunakan untuk memberikan hak istimewa kepada seseorang, agar dapat mengakses suatu data yang memiliki hak akses terbatas. Otorisasi juga sangat krusial pada komponen keamanan suatu sistem. Hal ini juga untuk menghindari kebocoran data yang diakibatkan oleh faktor *insider threat*, dimana hanya orang yang berwenang saja yang dapat mengakses data penting [11].

3. PERANCANGAN SISTEM

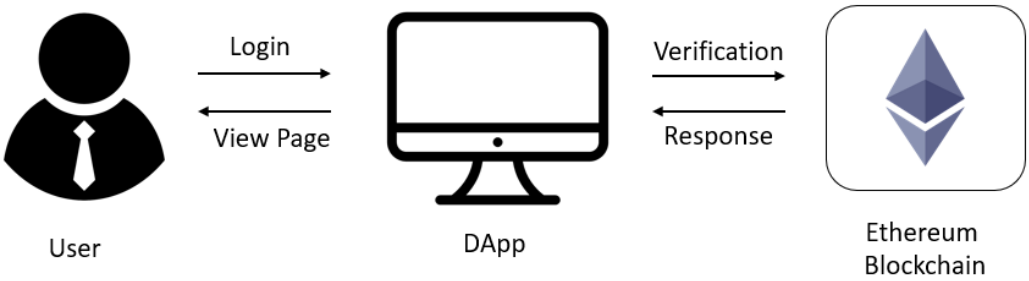
3.1. Perancangan Sistem

Aplikasi *web* yang akan dibangun akan memiliki tiga aktor, yaitu staff, ketua program studi (kaprodi), dan rektor. Staff memiliki akses untuk mengunggah dokumen ijazah dan transkrip nilai ke dalam *web*. Kaprodi memiliki akses untuk memberikan persetujuan kepada ijazah dan transkrip nilai pada *web*. Rektor juga memiliki akses untuk memberikan persetujuan setelah kaprodi menyetujui ijazah dan transkrip nilai.



Gambar 1 Use Case Diagram Aplikasi Web

Pengaturan hak akses akan menggunakan *Ethereum Blockchain* sebagai media penyimpanan. Aplikasi *web* yang dibangun menggunakan *Distributed Application* (DApp) dengan bantuan web3js. Dengan menggunakan web3js ini memungkinkan untuk dapat berinteraksi dengan *Ethereum Blockchain*. Pada saat *user* melakukan *login* sistem akan melakukan pengecekan terhadap *hash* data *user* pada *block* yang ada pada *Ethereum*. Apabila *hash* terverifikasi, maka *user* akan diarahkan ke halaman yang sesuai dengan pengaturan hak akses sebelumnya.



Gambar 2 Gambaran Sistem Aplikasi *Web* yang Akan Dibangun

3.2. Proses Pengujian

Proses pengujian adalah dengan melakukan serangan keamanan kepada sistem yang dibangun. Serangan yang dilakukan adalah untuk menguji tingkat keamanan dari sistem dalam segi integritas dari data kontrol akses yang ada pada *blockchain*, karena apabila serangan dapat dilakukan, maka data pengguna yang ada pada sistem dapat dilakukan perubahan kewenangannya.

Langkah-langkah yang dilakukan adalah sebagai berikut:

1. Buka halaman *login* dan masuk sebagai *SuperAdmin*. Lalu, melakukan registrasi untuk *user* baru. Jika berhasil, maka data akan masuk ke dalam *blockchain*.
2. Pengujian serangan, serangan dilakukan menggunakan *SQL Injection* pada form *input* dihalaman *login* dan halaman *user* dengan menggunakan parameter pada URL. Serangan *SQL Injection* yang dilakukan menggunakan *tools sqlmap*
3. Jika serangan berhasil dilakukan, maka dapat diasumsikan bahwa akan terlihat struktur dari *blockchain* yang menyimpan data-data yang tersimpan, sehingga dapat dilakukan serangan lanjutan untuk mengetahui *value* dari data yang ada.

DAFTAR PUSTAKA

[1]	Prasetiadi, A. E. (2020). Web 3.0: Teknologi Web Masa Depan. *Jurnal Industri Elektro dan Penerbangan*, *1*(3).
[2]	Andersen, M. P., Kolb, J., Chen, K., Fierro, G., Culler, D. E., & Popa, R. A. (2017). Wave: A decentralized authorization system for iot via blockchain smart contracts. *University of California at Berkeley, Tech. Rep*.
[3]	Ru, R., Selo, S., & Widyawan, W. (2017). Implementasi *Role-Based Access Control* (RBAC) pada Pemanfaatan Data Kependudukan Ditingkat Kabupaten. *Prosiding Semnastek.*
[4]	OWASP. "SQL Injection." owasp.org. https://owasp.org/www-community/attacks/SQL_Injection (Diakses Oktober 5, 2020).
[5]	Riadi, I., Umar, R., & Sukarno, W. (2018). Vulnerability of Injection Attacks Against The Application Security of Framework Based Bebsites Open Web Access Security Project (OWASP). *J. Inform*, *12*(2), 53-57.
[6]	Yunus, M. A. M., Brohan, M. Z., Nawi, N. M., Surin, E. S. M., Najib, N. A. M., & Liang, C. W. (2018). Review of SQL Injection: Problems and Prevention. *JOIV: International Journal on Informatics Visualization*, *2*(3-2), 215-219.
[7]	Crosby, M. (2015). *Blockchain* Technology Beyond *Bitcoin*. [*online*] Available at: https://scet.berkeley.edu/wp-content/uploads/*Blockchain*Paper.pdf [Accessed 7 Oct. 2020].
[8]	Carlozo, L. (2017). What is blockchain?. *Journal of Accountancy*, *224*(1), 29.
[9]	Gencer, A. E., Basu, S., Eyal, I., Van Renesse, R., & Sirer, E. G. (2018, February). Decentralization in bitcoin and ethereum networks. In *International Conference on Financial Cryptography and Data Security* (pp. 439-457). Springer, Berlin, Heidelberg.

[10]	Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*, *3*(37).
[11]	Claycomb, W. R., Huth, C. L., Flynn, L., McIntire, D. M., Lewellen, T. B., & Center, C. I. T. (2012). Chronological Examination of Insider Threat Sabotage: Preliminary Observations. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *3*(4), 4-20.
[12]	Aini, Q., Rahardja, U., Madiistriyatno, H., & Setiaji, Y. D. M. (2018). Pengamanan Pengelolaan Hak Akses Web Berbasis *Yii Framework*. *Syntax: Jurnal Informatika*, *7*(1), 52-63.
[13]	Noorsanti, R. C., Yulianton, H., & Hadiono, K. (2018). Blockchain-Teknologi Mata Uang Kripto (*Crypto Currency*).
[14]	Putri, M. C. I., Sukarno, P., & Wardana, A. A. (2020). *Two factor authentication framework based on ethereum blockchain with dApp as token generation system instead of third-party on web application*. Register: Jurnal Ilmiah Teknologi Sistem Informasi, 6(2), 74-85.