p-ISSN: 2655-8807
e-ISSN: 2656-8888

Manajemen Kontrol Akses Berbasis Blockchain untuk Pendidikan Online Terdesentralisasi

Nuke Puji Lestari[1]
Yusuf Durachman[2]
Srie Watini[3]
Shofiyul Millah[4]

Program Studi Sistem Informasi, Universitas Raharja Tangerang, Indonesia[1,4]
Program Studi Sistem Informasi, UIN Syarif Hidayatullah Jakarta, Indonesia[2]
Program Studi Pendidikan Anak Usia Dini, Universitas Panca Sakti, Indonesia[3]

Email: nuke@raharja.info[1], yuduf_daruchman@uinjkt.ac.id[2] , srie.watini@gmail.com[3]
shofiyul@raharja.info[4]

Notifikasi Penulis
19 Juli 2021
Akhir Revisi
20 Juli 2021
Terbit
01 Agustus 2021

Lestari, N. P., Durachman, Y., Watini, S., & Millah, S. (2021). Manajemen Kontrol Akses Berbasis Blockchain untuk Pendidikan Online Terdesentralisasi. *Technomedia Journal*, *6*(1).

https://doi.org/10.33050/tmj.v6i1.1682

ABSTRAK

Banyak pengguna menggunakan internet sebagai alat untuk layanan informasi yang lebih baik di lembaga pendidikan. Jaringan ini tidak memiliki penyedia layanan yang bertindak sebagai otoritas pusat dan pengguna memiliki kontrol lebih besar atas informasi mereka sehingga tidak ada pihak ketiga. Sehingga diusulkan sebagai solusi alternatif untuk sistem pembelajaran jaringan terpusat saat ini menggunakan Decentralized Online Educations (DOE). Banyak DOE telah diusulkan, namun keberadaan layanan Decentralized Online Educations (DOE) membutuhkan solusi terdistribusi yang efisien untuk melindungi privasi pengguna. Dalam beberapa tahun terakhir, banyak teknologi blockchain telah diimplementasikan ke dalam sistem pembelajaran sehingga sangat cocok untuk institusi pendidikan yang digunakan untuk menyelesaikan masalah privasi dalam sistem desentralisasi. Pada platform ini, menggunakan teknologi blockchain sebagai sistem penyimpanan, dan materi pembelajaran yang bersifat publik. Dalam studi ini, buat kerangka kerja kontrol akses yang dapat dikelola dan diaudit untuk Decentralized Online Educations (DOE) menggunakan teknologi blockchain untuk membahas definisi kebijakan privasi. Kunci publik yang digunakan oleh pemilik sumber daya menggunakan dari subjek untuk menentukan kebijakan akses dapat diaudit menggunakan Access Control List (ACL), sedangkan untuk mendekripsi data pribadi setelah izin akses divalidasi di blockchain menggunakan kunci pribadi yang terkait dengan akun Ethereum subjek. Untuk memberikan evaluasi dari pendekatan ini, gunakan testnet Rinkeby Ethereum untuk mengimplementasikan Kontrak Cerdas. Dan hasil dari percobaan ini dapat menunjukkan bahwa Access Control List (ACL) yang diusulkan menggunakan Attribute-Based Access Control (ABAC) dalam sistem pembelajarannya. Untuk mewujudkannya, diperlukan Access Control List (ACL).

Kata kunci : Pendidikan, Blockchain, Desentralisasi

p-ISSN: 2655-8807
e-ISSN: 2656-8888

ABSTRACT

Many users use the internet as a tool for better information services in educational institutions. This network has no service provider acting as a central authority and users have more control over their information so there are no third parties. So it has been proposed as an alternative solution for the current centralized network learning system using Decentralized Online Educations (DOE). Many DOEs have been proposed, but the existence of Decentralized Online Educations (DOE) services requires an efficient distributed solution to protect user privacy. In recent years, a lot of blockchain technology has been implemented into learning systems so that it is very suitable for educational institutions that are used to solve privacy problems in a decentralized system. On this platform, using blockchain technology as a storage system, and learning materials that are public. In this study, build a manageable and auditable access control framework for Decentralized Online Educations (DOE) using blockchain technology to address the definition of privacy policies. The public key used by the resource owner using from the subject to determine the access policy can be audited using the Access Control List (ACL), while to decrypt the private data after the access permission is validated on the blockchain using the private key associated with the subject's Ethereum account. To provide an evaluation of this approach use the Rinkeby Ethereum testnet to implement the Smart Contract. And the results of this experiment can show that the proposed Access Control List (ACL) uses Attribute-Based Access Control (ABAC) in the learning system. To make it happen, an Access Control List (ACL) is needed.

Keywords: Educations, Blockchain, Decentralized

PENDAHULUAN

Seiring dengan banyaknya kemajuan perkembangan informasi saat ini, jutaan orang menggunakan situs teknologi informasi untuk memenuhi kebutuhan sehari-hari karena teknologi informasi merupakan media yang tidak mengenal antar negara. Untuk meningkatkan kualitas dan kuantitas pendidikan, diperlukan sistem ketatanegaraan untuk menjadikan lulusan yang terbaik dan siap bersaing secara global [1]. Banyak orang yang tertarik pada jaringan online karena pelayanannya yang cepat dan lebih efisien, juga memiliki kepercayaan pada penyedia untuk memastikan kontrol akses untuk melindungi data sensitif pribadi mereka, seperti profil siswa, data siswa, dan hal-hal lain yang diposting secara publik. Dalam jaminan privasi pendidikan yang tidak dapat diprediksi saat ini, pengguna online mencari teknik berbagi data alternatif yang memungkinkan mereka untuk mendapatkan kendali atas data mereka sendiri (yaitu, memungkinkan mereka untuk mengelola data mereka sendiri) sambil membatasi dukungan penyedia layanan utama dalam mengendalikan data pribadi mereka sendiri [2]. informasi. Solusi Pendidikan Daring Terdesentralisasi (DOE) telah diusulkan untuk memenuhi kebutuhan ini, mulai dari P2P terdesentralisasi hingga sistem hibrida yang menggabungkan sumber daya pribadi dan eksternal untuk menyimpan data pengguna. Pendidikan Online Terdesentralisasi (DOE) adalah kerangka kerja yang memungkinkan layanan jaringan pendidikan dalam lingkungan terdistribusi. Karena karakter P2P dinamis dari DOE, diperlukan mekanisme kontrol akses yang ringan dan terdistribusi. Karena lingkungan DOE yang sangat dinamis, tugas terbuka hari ini di domain ini termasuk memastikan ketersediaan data, mendefinisikan metode kontrol akses yang ringan dan menjaga privasi, dan mengembangkan algoritme yang dapat diterima untuk penyebaran informasi dalam konteks terdistribusi [3]. Desain Pendidikan Online Terdesentralisasi (DOE) telah diusulkan dengan berbagai cara. Mayoritas dari mereka menggunakan enkripsi untuk memastikan privasi, dengan hanya

p-ISSN: 2655-8807
e-ISSN: 2656-8888

sebagian kecil yang mengandalkan kepercayaan untuk memberikan privasi. Beberapa strategi telah disajikan untuk memastikan pelestarian privasi di Decentralized Online Educations (DOE) [4]. Teknik seperti Kontrol Akses Berbasis Atribut (ABAC), Kontrol Akses Berbasis Peran (RBAC), dan kontrol akses berbasis aturan telah dikembangkan untuk meningkatkan tingkat privasi dan memastikan lebih banyak kontrol atas data [5]. Mengingat penggunaan media pendidikan saat ini, strategi ini tidak dapat menciptakan mekanisme yang terukur, terkelola, dan efisien untuk memenuhi kebutuhan keamanan Decentralized Online Educations (DOE) [6]. Sifat jaringan yang tersebar, kebutuhan untuk mengelola data pribadi pengguna yang tidak dapat disimpan di mana pun di jaringan, dan ketersediaan data adalah masalah utama dalam Decentralized Online Educations (DOE) [7]. Dalam DOE saat ini, pendekatan kontrol akses memerlukan penggunaan node online untuk menilai akses. Seperti yang disebutkan dalam generasi baru Decentralized Online Educations (DOE) yang menggabungkan teknologi blockchain [8], [9]. Jaringan Pendidikan Online berbasis Blockchain saat ini, di sisi lain, terutama dirancang untuk mengatasi masalah berita palsu dan untuk memberi kompensasi kepada pengguna untuk materi yang berharga [10]. Informasi pribadi biasanya direkam di blockchain dan diekspos ke semua orang jika opsi privasi dinonaktifkan. Sebuah pertanyaan mendasar muncul: bagaimana kita dapat menggunakan fitur teknologi blockchain untuk membangun skema kontrol akses yang dapat diaudit dan dapat dipercaya untuk Decentralized Online Educations (DOE)? Memang, platform Ethereum yang populer (yaitu, kontrak pintar) dan teknologi blockchain yang akan datang dapat dimanfaatkan untuk mengatasi masalah yang sulit ini [11]. Dalam penelitian ini, mengusulkan jaringan pendidikan terdesentralisasi berbasis blockchain yang menggunakan informasi konteks untuk menentukan kebijakan privasi dan menggunakan blockchain sebagai alat untuk pelestarian privasi [12]. Solusi yang disarankan unik karena menggunakan model ACL untuk menggunakan blockchain sebagai dasar untuk kontrol akses dalam situasi Decentralized Online Educations (DOE) . Demi kesiapan, sistem yang disarankan mengeksploitasi langkah-langkah kontrol akses, khususnya peraturan privasi, dengan bantuan blockchain, untuk memperhitungkan karakteristik utama dari Decentralized Online Educations (DOE) [13]. Proses penyimpanan material ini digunakan sebagai alat dengan menawarkan mekanisme kontrol akses yang aman [14].

PERMASALAHAN

Penelitian di bagian ini, memberikan solusi berbasis blockchain yang memberikan gambaran tentang arus Desentralisasi online Educations (DOE) yang digunakan untuk menjelaskan perkembangan dunia pendidikan. Selain itu, dapat memberikan informasi terbaru tentang kontrol akses dan memberikan ringkasan solusi yang diusulkan untuk menjelaskan kontribusi makalah ini [15]. Jaringan pendidikan online terdesentralisasi perbedaan mendasar antara konsep Decentralized Online Educations (DOE) saat ini adalah dalam penyimpanan data serta teknologi dalam proses pembelajaran. Usulkan klasifikasi yang memperhitungkan perbedaan-perbedaan ini [16]. Pendidikan Online Terdesentralisasi (DOE) di mana pengguna menyediakan server yang dikelola sendiri dan memungkinkan profil pengguna untuk ditempatkan di server mereka yang merupakan salah satu solusi terdesentralisasi pertama. Beberapa aplikasi penelitian telah diusulkan untuk Decentralized Online Educations (DOE) yang sepenuhnya terdesentralisasi adalah desain tiga tingkat dengan privasi, integritas, dan ketersediaan pada intinya [17]. Matryoshka adalah struktur konsentris logis yang dimiliki setiap pengguna. Matryoshka adalah cincin simpul konsentris yang terbentuk di sekitar setiap rekan yang memungkinkan penyimpanan data yang aman dan kebingungan komunikasi tidak langsung. PeerSon adalah arsitektur dua tingkat di mana Tabel Hash Terdistribusi (DHT) mengimplementasikan satu tingkat dan berfungsi sebagai layanan pencarian. Data pengguna,

p-ISSN: 2655-8807
e-ISSN: 2656-8888

seperti profil pengguna, disimpan di lapisan kedua, yang terdiri dari rekan-rekan. My3 adalah privasi ramah DOE yang memanfaatkan aspek menarik yang terkenal dari Jaringan Pendidikan Online, seperti kedekatan dan kepercayaan pengguna [18]. Profil pengguna disimpan secara eksklusif dalam kumpulan node tepercaya yang dipilih sendiri yang dikenal sebagai Trusted Proxy Set (TPS). Lokasi geografis pengguna dan jangka waktu online digunakan untuk memenuhi ketersediaan dan tujuan kinerja. DiDi SoNet adalah sistem dua tingkat di mana DHT mengimplementasikan tingkat yang lebih rendah dan overlay pendidikan digunakan untuk menerapkan tingkat yang lebih tinggi. Dalam overlay pendidikan, node terkait dengan node lain dengan siapa mereka memiliki kekuatan ikatan yang lebih kuat berdasarkan keterlibatan mereka. Hanya node tepercaya yang menyimpan data pendidikan, dan setiap node dapat memilih dua replika untuk memastikan tingkat keamanan yang tinggi. Untuk meningkatkan kualitas layanan pendidikan, beberapa DOE menghubungkan lapisan P2P dengan sumber daya eksternal seperti layanan penyimpanan cloud. Sumber daya eksternal digunakan untuk menangani kasus di mana pengguna tidak dapat menyediakan layanan mereka sendiri.

METODOLOGI PENELITIAN

A. Jaringan Pendidikan Online Berbasis Teknologi Blockchain

Beberapa Jaringan Pendidikan Online berbasis Blockchain (BOSN) telah diusulkan dalam beberapa tahun terakhir [19]. Platform ini bermaksud menggunakan teknologi blockchain untuk mengatasi tantangan privasi dan media pembelajaran palsu, serta memberikan nilai yang lebih besar pada materi dengan membangun sistem penghargaan. Dukungan untuk penyesuaian dan penyediaan konten berbayar tanpa memerlukan otoritas pusat adalah dua elemen platform yang menarik. Ia juga memiliki cryptocurrency yang disebut SPN, yang sesuai dengan ERC20. Untuk membedakan dirinya, NES menggunakan teknik konsensus bukti nilai. Untuk membedakan informasi berkualitas tinggi dalam jaringan, NES menggunakan teknik konsensus bukti nilai [20].

B. Model kontrol akses

Pendekatan Kontrol Akses Berbasis Peran (RBAC) memungkinkan pengguna untuk mendapatkan akses ke sumber daya berdasarkan tanggung jawab mereka dan mematuhi prinsip-prinsip seperti pemilihan tugas, hak istimewa terendah, dan pembagian fungsi administratif. Pendekatan RBAC dasar, di sisi lain, rentan terhadap masalah ledakan peran, sehingga tidak cocok untuk menerapkan kebijakan kontrol akses yang melibatkan skenario DOSN yang kompleks. Masalah ledakan peran adalah salah satu masalah yang paling umum ketika menerapkan RBAC dalam jaringan terdistribusi. Dalam lingkungan seperti itu, solusi seperti manajemen diri dapat digunakan untuk memecahkan masalah ledakan peran. Model Kontrol Akses Berbasis Atribut (ABAC) baru telah dibuat untuk membuat kebijakan kontrol akses terperinci dan memecahkan masalah ledakan peran dalam pengaturan jaringan terdistribusi, untuk mengatasi kendala model RBAC dalam pengaturan jaringan terdistribusi (yaitu, untuk mengurangi jumlah aturan yang terkait dengan model RBAC). Untuk menentukan kebijakan kontrol akses, model ini mempertimbangkan beberapa atribut seperti atribut subjek. Akibatnya, AC dapat mengeluarkan izin akses berdasarkan sertifikat atribut pengguna. Dalam sistem OSN dan DOE, otorisasi dan kontrol akses ke data pribadi merupakan fitur penting. Kebijakan akses ditentukan oleh OSN pada kepercayaan pengguna atau kekuatan mereka. Komponen kontrol akses di DOE harus responsif terhadap dinamika jaringan. Dalam sistem OSN dan DOE, otorisasi dan kontrol akses ke data pribadi merupakan fitur penting. Kebijakan akses ditentukan oleh OSN pada kepercayaan pengguna atau kekuatan mereka. Komponen kontrol akses di DOE harus responsif terhadap dinamika

p-ISSN: 2655-8807
e-ISSN: 2656-8888

jaringan. Karena satu titik kegagalan server, pendekatan ini tidak dapat digunakan dalam pengaturan yang terdesentralisasi. Sebaliknya, karena sesuai dengan keadaan di mana pemilik sumber daya menentukan hak atas sumber daya mereka, daftar kontrol akses (ACL) adalah metodologi umum untuk menerapkan kebijakan kontrol akses. DOE mendapat manfaat dari ACL karena menyediakan metode yang sangat rinci yang memungkinkan pengguna untuk membatasi materi pembelajaran sensitif ke beberapa teman mereka. ACL terdiri dari daftar satu atau lebih mata pelajaran serta seperangkat aturan. Setiap topik ditautkan ke operasi yang dapat dilakukan subjek pada sumber daya. Serangkaian aturan kriteria di mana satu atau lebih topik dalam daftar subjek harus mendefinisikan operasi secara terpisah. Pemilik sumber daya menggunakan ACL untuk subjek dengan sumber daya satu-ke-satu. Jika subjek atau grup yang memiliki subjek ditentukan dalam ACL yang terkait dengan sumber daya, subjek atau grup tersebut melakukan operasi pada sumber daya tersebut. ACL juga berisi informasi tentang metode akses yang diizinkan untuk digunakan subjek pada sumber daya. Dengan mendaftar entri terkait yang mewakili kebijakan berbasis ACL yang ada, akses ke sumber daya dapat dengan cepat dicabut. Dengan memanfaatkan properti teknologi blockchain, pembentukan kontrol akses berbasis blockchain untuk DOE dapat membantu mengatasi masalah perlindungan privasi dari sistem ini. Konsep serupa disajikan, tetapi penulis menggunakan blockchain sebagai server tepercaya untuk menyediakan fungsi kontrol pusat termasuk identitas pengguna, pemberitahuan umpan berita, dan rekomendasi teman. Dengan memanfaatkan properti teknologi blockchain, pembentukan kontrol akses berbasis blockchain untuk DOE dapat membantu mengatasi masalah perlindungan privasi dari sistem ini. Konsep serupa disajikan di, tetapi penulis menggunakan blockchain sebagai server tepercaya untuk menyediakan fungsi kontrol pusat termasuk identitas pengguna, pemberitahuan umpan berita, dan rekomendasi teman.

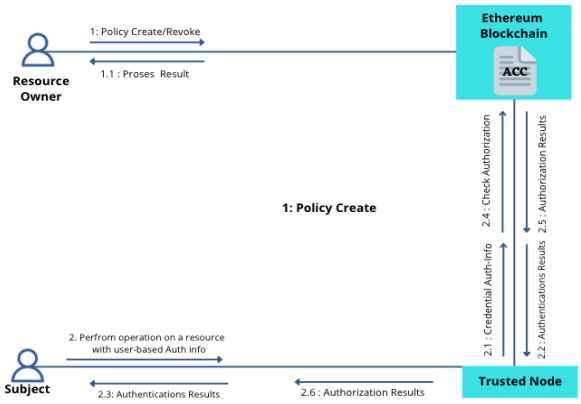
- Implementasi kontrol akses yang digerakkan oleh pengguna dan andal untuk DOE dalam skenario terdistribusi tetap menjadi masalah penelitian yang sulit.
- Kontrol akses yang cermat harus menangani sumber daya pengguna (seperti data, dan file siswa) dan informasi konteks.
- Tanpa bantuan otoritas pusat atau pihak ketiga yang tepercaya, sumber daya harus dilindungi dengan cara yang digerakkan oleh pengguna.
- Mekanisme kontrol akses harus dapat disesuaikan, memungkinkan pengguna untuk menetapkan izin yang berbeda untuk tugas yang berbeda seperti melihat, mengunduh, membaca, dan menulis, antara lain.
- Kontrol akses harus dapat dikontrol, memungkinkan pengguna untuk mengubah kebijakan yang ada yang disimpan di blockchain.
- Kebijakan yang telah dibuat harus dapat dibatalkan oleh pemilik sumber daya. Dia hanya perlu membuat transaksi baru yang menjelaskan kebijakan yang perlu dicabut untuk menyelesaikan operasi ini.
- Pengguna DOE jaringan harus dapat menentukan kebijakan untuk satu pengguna, sekelompok pengguna, satu sumber daya, atau banyak sumber daya. Dengan kata lain, pengguna dapat menambahkan sekelompok pengguna untuk menyelesaikan tugas pada satu atau banyak sumber daya. Kontrol akses harus dibatasi dalam arti bahwa pengguna hanya dapat melakukan tindakan terkait kebijakan (yaitu pembuatan kebijakan, pembaruan, dan pencabutan) atas nama mereka sendiri dan bukan atas nama DOE pengguna jaringan lain.

  Persyaratan untuk kontrol akses DOE didasarkan pada kebutuhan dan keragaman pelanggan. Pilih daftar kontrol akses (ACL) karena keserbagunaannya dalam mendukung operasi terdistribusi. Aspek penting seperti kelompok/tim dan informasi konteks juga didukung oleh ACL. Perlu dicatat bahwa validasi hak akses dalam pendekatan ini dilakukan oleh banyak entitas (yaitu, node tepercaya), yang menghindari satu titik

p-ISSN: 2655-8807
e-ISSN: 2656-8888

masalah kegagalan yang muncul dengan entitas terpusat. Selanjutnya, informasi konteks seperti waktu akses dan lokasi sangat penting untuk membuat solusi kontrol akses yang terperinci. Akibatnya, pendekatan ini memungkinkan pengguna untuk membuat aturan keamanan berdasarkan aspek-aspek ini sambil juga mempertimbangkan fitur daftar persyaratan. Kontrol akses sensitif konteks adalah strategi keamanan yang mengontrol akses sumber daya dengan mempertimbangkan berbagai jenis informasi konteks. Beberapa pendekatan kontrol akses konteks-sadar, seperti informasi geografis, informasi temporal, dan lokasi dan waktu, telah dikembangkan dalam beberapa tahun terakhir. Namun, karena data konteks berisi informasi pribadi, mengumpulkan dan mendistribusikannya di DOE dapat mengakibatkan masalah privasi. Akibatnya, sistem kontrol akses yang sadar konteks harus menyertakan perlindungan privasi yang kuat untuk memastikan bahwa data pribadi pengguna tidak terkait dengan identitas mereka yang sebenarnya. Dalam makalah ini, kami melihat bagaimana blockchain dapat membantu DOE dengan memanfaatkan kontrak pintar untuk membuat mekanisme kontrol akses yang terdistribusi, dapat diaudit, digerakkan oleh pengguna, dan dapat diskalakan. Studi ini menyajikan sistem kontrol akses kontekstual baru berdasarkan kontrak pintar dan ACL. Dengan meninggalkan aplikasi dan layanan sistem pendidikan satu sama lain, blockchain telah menghilangkan kebutuhan akan otoritas pusat. Arsitektur ini menyediakan berbagai kontrak pintar, termasuk Access Control Contracts (ACC), yang dapat mengontrol akses ke sumber daya jaringan, Reputation Contracts (RC), yang dapat menyediakan sistem yang dapat dipercaya, dan Inspector Contracts (IC), yang dapat memeriksa perilaku pengguna. Resource Owner (RO), yang merupakan pemilik resource tertentu, node yang dipercaya oleh RO, dan subjek yang tertarik untuk melakukan berbagai operasi pada resource RO adalah aktor utama dalam sistem ini. Solusi ini memungkinkan RO menggunakan ACL untuk menetapkan hak akses ke sumber dayanya, mencegah node tepercaya menolak hak akses yang diberikan oleh ACL. Menggunakan ACC pribadinya, RO membuat kebijakan kontrol akses yang terperinci dan dapat diaudit berdasarkan ID subjek. Selain itu, metode ini memungkinkan pengguna untuk memeriksa blockchain kapan saja untuk melihat perkembangan hak akses mereka. Perlu dicatat bahwa siapa pun yang ingin melakukan operasi pada salah satu sumber daya RO harus membuktikan bahwa mereka memiliki ID unik yang digunakan oleh RO untuk menetapkan kebijakan pada blockchain. RO dalam DOE dapat mengirim transaksi ke Access Control Contract (ACC) pribadinya untuk menetapkan izin akses ke sumber daya. Selanjutnya, ACC menyertakan fungsionalitas yang diperlukan untuk melaksanakan tugas memvalidasi hak akses menggunakan daftar kebijakan yang dipublikasikan di blockchain. RO memiliki kumpulan node tepercaya tempat data disimpan untuk memastikan ketersediaan data bahkan saat pengguna offline. Artikel ini tidak membahas pemilihan node replika tepercaya. Saat RO online, permintaan umum dikirim ke sana; jika tidak, itu dikirim ke salah satu node tepercaya yang dipilih secara acak. Untuk mengelola akses ke sumber daya, setiap RO memiliki ACC pribadi unik yang digunakan di blockchain.

p-ISSN: 2655-8807
e-ISSN: 2656-8888



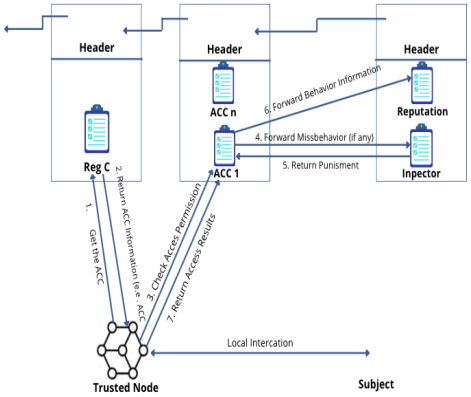
Gambar 1. **:** Ilustrasi pembuatan kebijakan, proses otentikasi dan otorisasi

Contract registrar (RegC) memberikan informasi tentang ACC RO ke node terpercaya. Node ini kemudian memvalidasi otorisasi akses untuk operasi yang diminta menggunakan ACC RO. Subjek diperbolehkan atau dilarang untuk melakukan operasi yang diinginkan pada sumber daya RO berdasarkan pemeriksaan regulasi kontrol akses. Perlu dicatat bahwa node tepercaya hanya memeriksa status otorisasi akses di blockchain, sedangkan RO menangani semua prosedur kepemilikan kebijakan seperti pembuatan, pembaruan, dan pencabutan kebijakan. Sistem kontrak pintar terdiri dari tiga kontrak pintar: Kontrak Kontrol Akses, Kontrak Inspeksi, dan Kontrak Reputasi[19]. Dalam proposal ini, masing-masing memainkan peran yang berbeda. Memang, RO dapat menggunakan ACC-nya sendiri untuk membatasi akses ke sumber daya jaringan; Kontrak Inspeksi memeriksa permintaan akses yang diberikan kepada ACC dan menghukum subjek yang tidak menghormati aturan ACC; Kontrak Reputasi (RepC) menghitung skor reputasi pengguna jaringan; dan Contract Registrars (RegCs) memungkinkan node tepercaya untuk menemukan informasi pengidentifikasi dari kontrak kontrol akses dan fungsi kontrol akses yang menyertainya. Di DOE, akses ke sumber daya dikonsolidasikan dan dikelola oleh server. Ada persyaratan untuk mencegah masalah privasi di DOE, dan dalam skenario khusus ini, perlu untuk memeriksa aktivitas pengguna secara terdesentralisasi. Karena dinamika jaringan dan kurangnya server pusat yang dapat memeriksa semua pengguna, fungsi penting ini sulit disediakan dalam sistem yang terdesentralisasi. Akibatnya, memutuskan untuk memasukkan skor reputasi dalam arsitektur yang menyoroti perilaku pengguna, dan setiap skor reputasi dipertahankan di blockchain dan dapat diakses publik berkat Kontrak Reputasi[20], [21]. Ini memastikan mekanisme kontrol akses yang andal. Perlu dicatat bahwa catatan reputasi terlihat di blockchain, sehingga memungkinkan pemilik sumber daya (RO) untuk mengecualikan pengguna dari daftar kebijakan jika mereka memiliki reputasi negatif di jaringan. Subjek akan diklasifikasikan sebagai tidak jujur karena berbagai alasan yang dijelaskan dan dimasukkan ke dalam sistem sebagai input. Misalnya, jika pengguna mengirim terlalu banyak permintaan untuk mengakses sumber daya RO, pengguna tersebut dapat dianggap tidak jujur. Frekuensi akses adalah parameter, dan harus memperhitungkan data pendidikan yang sebenarnya, seperti profil siswa. Frekuensi akses merupakan parameter sehingga perlu diperhatikan informasi pendidikan, seperti aktivitas siswa, yang dapat mengakses pembelajaran berkali-kali.

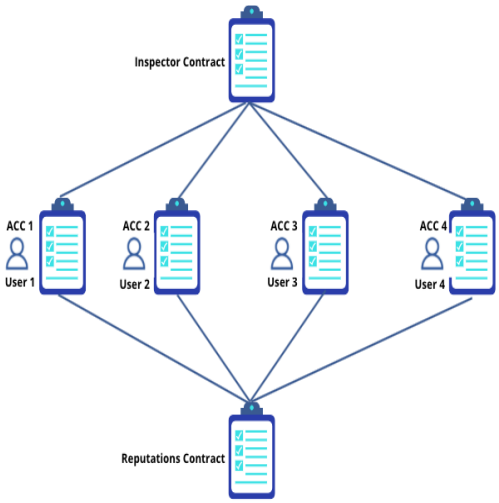
HASIL DAN PEMBAHASAN

p-ISSN: 2655-8807
e-ISSN: 2656-8888

Kami menyajikan gambaran penuh dari sistem kontrak pintar kami diusulkan di bagian ini, seperti yang diilustrasikan pada Gambar. 3.



Gambar. 2. Menunjukkan arsitektur berbasis blockchain untuk jaringan pendidikan online desentralisasi.



Gambar 3. Menunjukkan cara kerja kontrak pintar.

A. Kontrak untuk Kontrol Akses (ACC)

ACC adalah kontrak yang mengatur akses sumber daya.

Untuk mengelola akses ke sumber daya DOE, setiap RO memiliki ACC unik yang digunakan pada blockchain Ethereum. Dengan mengirimkan transaksi ke ACC-nya sendiri yang berisi informasi kebijakan, RO dapat membuat atau mengubah kebijakan kontrol akses. Selanjutnya, setiap ACC ditautkan ke daftar kebijakan, yang berisi informasi tentang aturan kontrol akses.[22] Tabel 1 mengilustrasikan contoh daftar kebijakan. Bagian berikut dari daftar kebijakan dieksplorasi secara rinci:

- Sumber daya: Bidang ini menentukan nama sumber daya yang perlu disertakan dalam prosedur kontrol akses.
- Subjek: Bidang ini menunjukkan id unik (yaitu, alamat Ethereum) dari subjek di jaringan DOE.
- Tindakan: Ini menentukan tindakan yang dapat dilakukan pada sumber daya tertentu, seperti melihat, mengunduh, membaca, dan menulis.
- Lokasi: Bidang ini berisi informasi tentang lokasi akses subjek.
- Rentang Waktu: RO dapat menggunakan bidang ini untuk mengatur rentang waktu untuk membatasi jumlah waktu pengguna memiliki akses ke sumber daya.

p-ISSN: 2655-8807
e-ISSN: 2656-8888

- Otorisasi: Bidang ini digunakan untuk menjelaskan izin mitra (sumber daya, subjek), seperti mengizinkan atau menolak.
- Waktu Permintaan Terakhir (LRT): Bidang ini melacak kapan permintaan terakhir dibuat.
- Waktu Permintaan Terakhir (LRT): Bidang ini menyimpan waktu permintaan akses terbaru dari subjek.

Demi kesederhanaan, kami akan menganggap bahwa setiap baris daftar kebijakan hanya berisi satu ID subjek. Di sisi lain, sistem yang diusulkan dapat disesuaikan karena aturan ACL dapat disesuaikan untuk menggabungkan beberapa tema. Bahkan, dalam satu transaksi, RO dapat membangun kebijakan berbasis ACL untuk beberapa topik[23]. Selain itu, RO dapat dengan mudah mencabut polis yang ada dengan mengirimkan transaksi pencabutan polis yang menyertakan informasi identitas polis yang dibatalkan. Perlu dicatat bahwa hanya RO yang memiliki wewenang untuk menggunakan fungsi utama ACC. Memang, pendekatan ini meningkatkan keamanan sistem kontrol akses karena, seperti yang dinyatakan sebelumnya di bagian persyaratan, sistem ingin dibatasi. Waktu tunggu untuk subjek yang terlibat dapat menjadi hukuman yang wajar dalam situasi ini[24]. Memblokir subjek seperti itu adalah salah satu konsekuensi yang mungkin terjadi dalam menghadapi situasi ini. Kontrak pintar Ethereum menyediakan Application Binary Interfaces (ABI) atau fungsi yang dapat digunakan untuk melakukan tugas terkait kebijakan dengan mengirimkan transaksi materi pembelajaran. Akibatnya, ACC yang diusulkan memungkinkan berbagai transaksi materi pembelajaran yang diperlukan untuk menjalankan ABI ini. Berikut ini adalah ikhtisar singkat dari berbagai fungsi ACC yang diusulkan:

- policy Add(): ACC menggunakan fungsi ini untuk membuat kebijakan baru pada pasangan sumber daya/subjek tertentu. Ketika fungsi ini dijalankan, kebijakan yang dihasilkan ditambahkan ke daftar kebijakan blockchain saat ini.
- policy Update(): Fungsi ini digunakan untuk memperbarui kebijakan yang telah ditentukan sebelumnya pada sumber daya tertentu, pasangan subjek. Harap perhatikan bahwa Anda dapat mengubah kebijakan kapan saja dengan mengubah ID subjek, informasi konteks, tindakan, otorisasi akses, atau kombinasi dari faktor-faktor ini.
- Pembaruan Lokasi : RO dapat menggunakan fungsi ini untuk mengubah lokasi akses yang disediakan dalam kebijakan berbasis ACL.
- Ini memerlukan informasi pengidentifikasian dari kebijakan yang memerlukan modifikasi lokasi. Selain itu, RO harus menunjukkan lokasi akses baru dan memulai transaksi untuk menggunakan fungsi Update() lokasi dari kontrak pintar ACC.
- Pembaruan Timeranger : RO dapat menggunakan fungsi ini untuk memperbarui bidang rentang waktu yang ada dalam kebijakan. Ini juga memerlukan informasi identifikasi kebijakan serta nilai rentang waktu baru untuk memperbarui nilai kebijakan yang ada.
- Penghapusan Kebijakan : Fungsi Hapus () kebijakan ACC dapat digunakan untuk menghapus kebijakan yang ada dari blockchain. RO harus memberikan informasi pengidentifikasi untuk kebijakan yang harus dihapus untuk mencapai tujuan ini. Fungsi ini digunakan oleh RO atau node tepercaya untuk memvalidasi kebijakan kontrol akses di blockchain. Harap dicatat bahwa untuk memvalidasi otorisasi akses di blockchain, hanya node tepercaya yang ditunjuk oleh RO di ACC yang mampu mengirim transaksi. Untuk mengidentifikasi izin yang terkait dengan kebijakan, fungsi ini juga memerlukan informasi identifikasi kebijakan (yaitu, ID subjek dan nama sumber daya), informasi konteks, dan waktu akses saat ini. Selain itu, fungsi ini tidak hanya mengevaluasi perilaku subjek dengan mempertimbangkan informasi konteks dan jumlah permintaan

p-ISSN: 2655-8807
e-ISSN: 2656-8888

berulang dalam waktu singkat, tetapi juga melakukan validasi statis kebijakan kontrol akses. Selain itu, fungsi ini tidak hanya melakukan validasi statis kebijakan kontrol akses, tetapi juga memeriksa perilaku subjek dengan mempertimbangkan informasi konteks dan jumlah permintaan berulang dalam waktu singkat. Akhirnya, jika permintaan akses memenuhi kriteria validasi statis dan dinamis, itu diperbolehkan.

- Nonaktifkan : Fungsi ini dapat digunakan untuk menonaktifkan ACC berbasis blockchain. Untuk sepenuhnya melepaskan penyimpanan yang ditempati oleh kode kontrak pintar ini, gunakan fungsi penghancuran diri.

B. Kontrak Inspektur (IC)

Saat permintaan akses diberikan kepada ACC, kontrak Inspektur menyelidiki perilaku subjek dan memeriksa komunikasi mereka. Saat membuat permintaan untuk melakukan prosedur atas aset, kami berasumsi bahwa subjek yang adil akan memperhatikan standar ACC. Subjek yang tidak bermoral, sekali lagi, bertindak aneh dengan mengganggu norma-norma ACC. Saat membuat permintaan untuk melakukan prosedur atas aset, kami berasumsi bahwa subjek yang sah akan memperhatikan prinsip-prinsip ACC. Subjek yang tidak bermoral, sekali lagi, bertindak secara khusus dengan mengganggu pedoman ACC. Kontrak Inspektur menggabungkan sistem penemuan gaduh yang menganalisis aktivitas subjek dan menurunkan disiplin yang bergantung pada jenis pembuatan masalah. Ketika ACC telah mengenali subjek sebagai meragukan, laporan dikirim dari perjanjian IC, yang melihat jenis kerusakan dan memilih disiplin yang sesuai sebelum mengembalikan data ke kontrak ACC. Akhirnya, ACC menyelesaikan persetujuan terhadap pelaku kesalahan[25]. *IC berisi ABI atau kapasitas khusus yang digunakan untuk melakukan survei subjek. Kapasitas ini mendapatkan informasi dari ACC, mengevaluasi nya, dan kemudian menetapkan suatu disiplin. Berikutnya adalah rincian dari beberapa kapasitas perjanjian:*

- inspect Behavior(): Kapasitas ini menilai informasi perilaku yang didapat dari ACC untuk memutuskan hukuman yang tepat. Ini mengevaluasi perilaku dan melaporkan kembali ke ACC tentang disiplin. Akhirnya, ACC mengimplementasikan pilihan organisasi DOSN pada isu yang berlaku.
- menonaktifkan (): ABI ini dapat dimanfaatkan untuk membunuh kontrak pemeriksa Kontrak blockchain ini

C. Reputasi (RepC)

Kepercayaan dewan kerangka mengizinkan hub untuk memutuskan apakah subjek diandalkan, memungkinkan ROS untuk mengimbangi atau penolakan subjek kemudian[26].*Untuk kerangka kerja terbuka yang besar, sistem kepercayaan dan ketenaran pada prinsipnya digunakan. Kedudukan individu atau spesialis biasanya merupakan nilai dunia yang menunjukkan karakter, (misalnya, adil, tidak bermoral, atau solid) dari elemen tersebut. Kepercayaan, sekali lagi, menunjukkan kesan yang berubah dari penilaian klien. Sebuah harga kepercayaan ditunjuk untuk pasangan tertentu dari klien untuk alasan kesiapan. Tidak diragukan lagi, keterlibatan klien sendiri dalam klien lain dapat mendorong kepercayaan. Seperti yang ditunjukkan oleh tinjauan tulisan, ada dua jenis kemasyhuran kerangka kerja dewan: disatukan dan terdesentralisasi. Seorang pekerja fokus, seperti pekerja awan, sesering mungkin digunakan dalam kerangka kerja terpadu untuk menyimpan dan menangani skor berdiri. Desentralisasi mempercayai pengaturan eksekutif, sekali lagi, pertimbangkan hub dalam organisasi saat menghitung dan menyimpan rekor berdiri*[27].

p-ISSN: 2655-8807
e-ISSN: 2656-8888

D. Kontrak Registrar (RegC)rahasia

- Kontrak Registrar digunakan untuk mengizinkan hub untuk menemukan data pengenalan untuk ACC dan pekerjaan kontrol akses yang menyertainya. Seperti yang ditunjukkan pada Tabel 4, perjanjian ini memantau catatan yang digunakan untuk melakukan kontrol penerimaan yang tersebar di organisasi, memberikan tahap kepada hub yang dipercaya untuk mencari data. Tentunya, ketika hub yang dipercaya telah mendapatkan data terkait, misalnya, ID ACC yang disebutkan dan pekerjaan kontrol akses yang berjalan, seperti yang ditunjukkan pada Tabel 4, ia dapat mengirim pertukaran untuk memeriksa persetujuan akses di blockchain. Ketika RO tidak dapat diakses atau perusahaan sedang down, subjek dapat mengirimkan permintaan masuk ke hub online terpercaya yang tidak resmi. Ketika RO tidak dapat diakses atau organisasi sedang down, subjek dapat mengirimkan permintaan masuk ke hub terpercaya online reguler. Saat membuat permintaan masuk ke hub yang dipercaya, subjek S harus menyatakan bahwa ia akan mendapatkan aset RO, di mana S dan RO adalah pengidentifikasi terpisah subjek dan RO. Mengikuti pernyataan data ini dalam permintaan masuk, hub yang diyakini menggunakan pengidentifikasi RO untuk mendapatkan ID ACC dan pekerjaan kontrol akses terkait yang diberikan oleh RO, seperti yang ditunjukkan pada Tabel 4. Hub yang diyakini mengirimkan pertukaran ke ACC yang diperlukan untuk periksa otorisasi akses di blockchain menggunakan ID subjek, ID ACC, dan kontrol masuk terkait ABI.
- ID RO: Bidang ini berisi data tentang ID pemilik ACC.
- ID ACC: Properti ini berisi id dari perjanjian tajam ACC yang telah diletakkan di blockchain.
- Kontrol Akses ABI: Bidang ini berisi data tentang ABI kontrol masuk perjanjian ACC.

KESIMPULAN

Menggunakan daftar kontrol akses, sistem kontrol akses yang dapat diaudit dan dapat dipercaya disarankan untuk DOE dalam penelitian ini (ACL). Di blockchain, pemilik sumber daya memiliki ACC pribadi unik yang digunakan untuk mengatur akses ke sumber daya jaringan. Solusi yang diusulkan terdiri dari berbagai kontrak pintar yang dimaksudkan untuk memenuhi persyaratan kepercayaan dan keamanan DOE. Karena semua fungsi yang dipanggil pada kontrak pintar dicerminkan pada blockchain Ethereum, metode yang disarankan dengan benar mencapai karakteristik kemampuan audit. Akibatnya, semua tindakan pengguna dapat dilihat secara publik di blockchain. Seorang pengguna tidak akan dapat melakukan aktivitas tersembunyi tanpa sepengetahuan pengguna lain. Selanjutnya, pengguna yang berwenang dapat mengakses sumber daya bahkan jika pemilik sumber daya (RO) tidak tersedia atau terputus. Karena protokol tantangan-tanggapan digunakan untuk melakukan verifikasi identitas pengguna yang aman dan untuk memverifikasi status otorisasi akses di blockchain, kami merekomendasikan sistem kontrak pintar yang mencapai properti verifikasi. Akhirnya, kami membangun dan menilai metodologi dengan menerapkan kontrak pintar pada testnet Rinkeby Ethereum, dan hasilnya menunjukkan bahwa teknik yang kami usulkan layak. Untuk menilai aturan ACL, teknik kami membutuhkan 61.648 gas.

SARAN

Sebagai pekerjaan di masa depan, peneliti berencana untuk mengevaluasi kerangka kerja kami dalam skenario DOE yang nyata, dan berencana untuk mempelajari lebih dalam masalah Kontrol Akses dengan membandingkan pendekatan kami dengan model lain yang

p-ISSN: 2655-8807
e-ISSN: 2656-8888

berbeda untuk menyoroti manfaat di DOE. Secara khusus, untuk menyelidiki perilaku lintas konteks subjek, serta perubahan pola perilaku dalam konteks tertentu

DAFTAR PUSTAKA

[1] F. P. Oganda, U. Rahardja, Q. Aini, M. Hardini, and A. S. Bist, "BLOCKCHAIN: VISUALIZATION OF THE BITCOIN FORMULA," *PalArch's Journal of Archaeology of Egypt/Egyptology*, vol. 17, no. 6, pp. 308–321, 2020.

[2] F. Agustin, S. Syafnidawati, N. P. Lestari Santoso, and O. G. Amrikhasanah, "Blockchain-based Decentralized Distribution Management in E-Journals," *Aptisi Transactions On Management*, vol. 4, no. 2, pp. 107–113, 2020.

[3] M. Hardini, Q. Aini, U. Rahardja, R. D. Izzaty, and A. Faturahman, "Ontology of Education Using Blockchain: Time Based Protocol," in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2020, pp. 1–5.

[4] Q. Aini, A. Badrianto, F. Budiarty, A. Khoirunisa, and U. Rahardja, "Alleviate Fake Diploma Problem In Education Using Block Chain Technology," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. 2, pp. 1821–1826, 2020, doi: 10.5373/JARDCS/V12I2/S20201225.

[5] C. Lukita, M. Hatta, E. P. Harahap, and U. Rahardja, "Crowd funding management platform based on block chain technology using smart contracts," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. 2, 2020, doi: 10.5373/JARDCS/V12I2/S20201236.

[6] U. Rahardja, Q. Aini, M. D. A. Ngadi, M. Hardini, and F. P. Oganda, "The Blockchain Manifesto," in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2020, pp. 1–5.

[7] E. P. Harahap, Q. Aini, and R. K. Anam, "PEMANFAATAN TEKNOLOGI BLOCKCHAIN PADA PLATFORM CROWDFUNDING," *Technomedia Journal*, vol. 4, no. 2, pp. 199–210, 2020.

[8] S. Kosasi, "Karakteristik Blockchain Teknologi Dalam Pengembangan Edukasi," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 1, no. 1, pp. 87–94, 2020.

[9] Q. Aini, N. Lutfiani, N. P. L. Santoso, S. Sulistiawati, and E. Astriyani, "Blockchain For Education Purpose: Essential Topology," *Aptisi Transactions on Management (ATM)*, vol. 5, no. 2, pp. 112–120, 2021.

[10] D. Cahyadi, A. Faturahman, H. Haryani, and E. Dolan, "BCS: Blockchain Smart Curriculum System for Verification Student Accreditation," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1, pp. 65–83, 2021.

[11] A. Maharani, S. Aninda, and S. Millah, "Pembuatan Kartu Ujian Online Sebagai Pengabdian Perguruan Tinggi," *ADI Pengabdian Kepada Masyarakat*, vol. 1, no. 2, pp. 8–14, 2021.

[12] Z. Fauziah, H. Latifah, X. Omar, A. Khoirunisa, and S. Millah, "Application of Blockchain Technology in Smart Contracts: A Systematic Literature Review," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 2, no. 2, pp. 160–166, 2020.

[13] R. Rosyid and M. A. W. Prasetyo, "Robot Peraga 12 Gerakan Pengaturan Lalu Lintas Berbasis Arduino Mega 2560," *Technomedia Journal*, vol. 5, no. 2, pp. 193–205, 2021.

[14] K. Nalakhudin, M. Imron, and M. A. W. Prasetyo, "Pemanfaatan Notifikasi Telegram Untuk Monitoring Perangkat CCTV Rumah Sakit Orthopaedi Purwokerto," *Technomedia Journal*, vol. 6, no. 01 Agustus, 2021.

[15] B. E. Sibarani, "Smart Farmer Sebagai Optimalisasi Digital Platform Dalam Pemasaran Produk Pertanian Pada Masa Pandemi Covid-19," *Technomedia Journal*, vol. 6, no. 01 Agustus, 2021.

[16] R. A. A. Rahman and A. Adhitya, "Perancangan Sistem Informasi Pengusulan Kenaikan Pangkat Berbasis Web Pada Korps Marinir TNI AL," *Technomedia Journal*, vol. 6, no. 01 Agustus, 2021.
[17] H. Sulistiani, A. Yuliani, and F. Hamidy, "Perancangan Sistem Informasi Akuntansi Upah Lembur Karyawan Menggunakan Extreme Programming," *Technomedia Journal*, vol. 6, no. 01 Agustus, 2021.
[18] T. Hariguna, Y. Durachman, M. Yusup, and S. Millah, "Blockchain Technology Transformation in Advancing Future Change," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 13–20, 2021.
[19] B. D. Wicaksono and S. Anggraeni, "Perancangan Website Sistem Informasi Transaksi Tagihan Layanan Purna Jual Properti Pada Pollux Properti Indonesia," *TMJ (Technomedia Journal) Vol. 5 No. 2 Februari 2021*, p. 132, 2021.
[20] N. Sany and M. Kurniawan, "Sistem Informasi Surat Masuk Pada Pengelolaan Rantai Suplai Satuan Kerja Khusus Migas," *TMJ (Technomedia Journal) Vol. 5 No. 1 Agustus 2020*, p. 27, 2021.