e-ISSN 2962-0651
JURNAL KOMPUTER

Blockchain-based Identity Management System: Desain dan studi Kemanan

Novi Rahayu [1)]
[1)]***STIA Bengkulu , Indonesia***
Email: [1)] novi@gmail.com

Abstrak

Internet of Things(IoT) adalah sejumlah perangkat yang dapat mengumpulkan dan mengirimkan data antar sensor tanpa perlu bantuan manusia. Namun, keamanan IoT dapat terancam karena sifatnya yang dapat diakses dari mana saja dan kapan saja.Celah keamanan memiliki kemungkinansukar untuk dideteksi, karena memiliki pola yang beragam.Oleh karena itu, diperlukan sebuah model keamanan pengiriman data antar sensor yang aman. Blockchain adalah teknologi yang dapat menjawab tiga syarat keamanan yang diperlukan, yaitu ketersediaan, kerahasiaan, dan integritas. Dalam penelitian ini, kami mencoba membangun sebuah simulasi keamanan IoT dengan menggunakan teknologi blockchain, dimana sistem keamanannya menggunakan pola publicblockchain. Metode yang digunakan dalam penelitian ini adalah model publicblockchain yang memungkinkan para pengguna untuk mengendalikan aplikasi yang terhubung pada pin emulatormelalui smart contract. Penelitian ini menggunakan jejaring Ethereum yang termasuk dalam jaringan pengujian yang dapat digunakan tanpa adanya biaya transaksi yang perlu dibayar. Dengan adanya penelitian ini, diharapkan dapat memberikan solusi pada permasalahan keamanan dan tantangan yang dihadapi dalam jaringan IoT

Kata kunci: *Blockchain, Internet Of Things(Iot), Simulasi,Keamanan,Smart* Contract.

Blockchain-Based Identity Management System: Design And Security Study

Abstract

The Internet of Things (IoT) is a number of devices that can collect and transmit data between sensors without the need for human assistance. However, the security of IoT can be threatened due to its nature that can be accessed from anywhere and at any time. Security gaps have the possibility of being difficult to detect, because they have a variety of patterns. Therefore, a secure model for sending data between sensors is needed. Blockchain is a technology that can answer the three necessary security requirements, namely availability, confidentiality, and integrity. In this research, we try to build an IoT security simulation using blockchain technology, where the security system uses the publicblockchain pattern. The method used in this research is a publicblockchain model that allows users to control applications connected to the emulator pin through smart contracts. This research uses the Ethereum network which is included in the testing network that can be used without any transaction fees that need to be paid. With this research, it is hoped that it can provide solutions to security problems and challenges faced in IoT networks.

Keywords*: Blockchain, Internet Of Things (Iot), Simulation, Security, Smart Contracts.*

PENDAHULUAN

Internet of Things(IoT) adalah sejumlah perangkat yang mampu mengumpulkan dan mengirimkan data antar sensor tanpa perlu bantuanmanusia (Ali et al., 2019). Namun,sifat IoT yang dapat diakses dari mana saja dan kapan saja, maka hal inidapatmenimbulkan ancamanpada keamanannya.Celah keamanan memiliki kemungkinansukar untuk dideteksi, karena memiliki pola yang beragam. Penyebabadanya ancaman pada keamanan bisa disebabkan oleh konfigurasi jaringan yang kurang tepat(Sidiq et al., 2020; Riadiet al., 2021). Prinsip dari aspek sistem keamanan

jaringan secara umumterdiridari tiga hal yaitu ketesediaan, kerahasiaan, dan integritas(Matondang et al., 2018;Pramudita et al., 2020; Sari et al., 2020).
Oleh sebab itu, pada penelitian ini kami menggunakan pin emulatorGPIO karena sifatnya yang sudah tersedia untuk digunakan. Selain itu, emulatorini banyak digunakan dalam penelitian lainnya dibandingkan dengan emulator lain yang masih jarang digunakan.Untuk pola integrasi blockhain dan IoT memanfaatkan pola integrasi assetke blockchain.Program yang dibangun kemudian dijalankan pada private networkkemudianpengguna dapat melihat status setiap pin pada baris perintah dan juga pada emulator.Penelitian seperti ini sudah pernah dilakukan sebelumnya: penelitian yang dilakukan oleh Puri et al. (2021)menghasilkan pendekatan yang diusulkan untuk menunjukkan kinerja yang memuaskan dan performa yang berhubungan dengan bandwidthdan konsumsi daya. Dalam penelitian kami memiliki kesamaan dengan penelitian yang dilakukan oleh Puri et al. dimana kami ingin melihat kinerja konsumsi daya. Tetapi pada penelitian kami juga akan melihat transaksi dan block timepada saat transaksi dilakukan. Selain itu, penelitian Baccelli et al. (2018)menghasilkan ketersediaan sistem operasi yang open sourceuntuk perangkat Low-end Embeddeddalam IoT seperti RIOT. Dalam penelitian ini menggunakan GPIO sebagai micro controller.

Pada penelitian kami, kami menggunakan pinemulator GPIO tetapi kami juga mengintegrasikan GPIO dengan controllerberbasis web agar pengguna dapat menggunakan controlleryang lebih mudah dipahami untuk memberikan interupsi terhadap pin pada emulator.Penggunaan blockchain pada simulasi keamanan IoT melalui pin emulatoradalah untuk mengevaluasi kelayakan keamanan sebelum penerapan yang sebenarnyadilakukan. Selain itu, kami menggunakan simulatoragar dapat mensimulasikan leader, server, dan perangkat untuk generatedan mengirim transaksi. Dengan menggunakan blockchain maka perangkat dapat mengumpulkan dan bertukar data dengan server, perangkat lain, maupun platformlainnya. Keuntungan dari blockchain untuk meningkatkan sistem IoT adalah: desentralisasi, verifikasi kolektif dan ketahanan terhadap gangguan, keamanan pribadi, kecepatan, penghematan biaya, dan smart contract(Zhou et al., 2018; Atlam et al., 2018).

Pada penelitian ini, kami mengadopsi model publicblockchain, dimana setiap pengguna yang memiliki akses internet dan akses aplikasinya dapat melakukan transaksi pada setiap aplikasi yang terhubung dengan mengendalikan pin emulatorGPIO (turning onatau turning off) melalui smart contract. Dengan begitu,para pengguna dapat mengontrol aplikasi yang terhubung pada pin emulator. Selain itu, penelitian ini menggunakan jejaring Ethereum yang termasuk dengan jaringan pengujian yang dapat kami gunakan tanpa adanya biaya transaksi yang perlu dibayar (Sidiqet al., 2020). Dasar penggunaan model publicblockchain pada penelitian ini karena bersifat anonymous. Meskipun data yang digunakan tersimpan pada jaringan puclicblockchain bersifat transparan atau dapat dilihat oleh pihak lain. Namun, untuk identitas setiap pengguna yang mengirim atau menerima data transakasi tidak dapat diketahui oleh pihak lainnya.

LANDASAN TEORI

Blockchain adalah teknologi yang mampu menjawab tiga syarat keamanan yang di perlukan yaitu ketersediaan, kerahasiaan dan integritas.Blockchain adalahteknologi baru yang awalpenerapannya pada bitcoin(Nakamoto, 2008), yang terus berkembang dengan cepat dalam satu dekade ini(Huang et al., 2021). Blockchain pada dasarnya adalah sistem basis data terdistribusi yang menyimpan data transaksional yang diamankan oleh kriptografi(Taylor et al., 2020). Selain itu, blockchain menggunakan kriptografi saat memproses serta memverifikasi sebuah proses transaksi. (Coleet al.,2019).Enkripsi dan pengkodean data dalam blockchain meningkatkan transparansi, efisiensi dan kepercayaan dalam berbagi data dan informasi.Dibeberapa bidang, teknologi blockchain telah mempengaruhi dan memberikan manfaat dibidang pertanian(Wihartiko et al., 2021), kesehatan, farmasi(Fernandoet al., 2020), ekonomi, industry (Helliaretal., 2020)dan bidang lainnya.

Terkhusus dalam bidang teknologi, yaitujaringan untuk IoT dan sensor.Dimana manajemen dan pengaturan IoT menggunakan private blockchain(Košťál et al., 2019; Lockl et al., 2020). Sistem keamanan mengusulkan sebuah private blockchain-basedaccess controlyang melibatkan penggunaan privateblockchain dalam menyediakan keamanan dasaryang tidak bisa di manipulasi (Xue et al., 2018).Sehingga memberikan tantangan tersendiri dalam menghadirkan keamanan dan solusi pada permasalahan jaringan IoT(Singhet al., 2021).Dalam penelitian ini, kami mencoba untuk membangun sebuah simulasi keamanan IoT,dimana sistem keamanannya menggunakan teknologi blockchain dengan mengambil pola publicblockchain. Akses aplikasi dibangun menggunakantext editorVisual Studio Codedan dikendalikandengan menggunakanpin emulatorGPIO. Pin emulatorGPIO memiliki fungsi untuk membaca status pin, mengatur/menghapus pin, dan menjalankan panggilan balik setelah

e-ISSN 2962-0651
JURNAL KOMPUTER

interupsi pin(Feng et al., 2020). Dalam penelitian kami, kami mengamati setiap pin dalam melakukan transaksi data. Python sudah menyediakan packagepin emulatorGPIO yang siap digunakan dengan cara menginstal menggunakan pip.

METODE PENELITIAN

Model Blockchain

Penggunaan blockchain untuk sebuah keamanan mengacu pada satu set penambang terdesentralisasi yang menjalankan protokol konsensus yang aman.Konsensus padablockchain yang didistribusikandantidak dapat dipercaya, maka dapat dianggap Byzantine Generals Problem(BGP). Jika hal ini terjadi, maka pembuat programkemudian bertanggung jawab untuk memvalidasi kembali blok baru dan mendistribusikan melalui jaringan yang telah ditetapkan. Dalam penelitian ini, kami menggunakan mekanisme konsensus Proof of Stake(PoS). PoS digunakan untuk bukti pertaruhan assetcryptodalam Ethereum. Pada tabel 1 memperlihatkan perbandingan protokol konsensusyang adapada blockchain(Panarello et al., 2018).Selain mempertahankan buku besar(public ledger)global untuk keseimbangan disetiap nama samaran, blockchain juga dapat mengeksekusi program yang telah dibuat dan ditentukan oleh pengguna. Seperti waktu, negara bagian publik,pengiriman pesan,nama samaran,kebenaranserta ketersediaannya(Kosba et al., 2016).

Perancangan Program

Pada program yang dibuat dijalankan dengan menggunakan GPIOemulator, terminal (Command Prompt pada Windows) dan juga controlleruntuk pinyang berbasis websiteuntuk antar-muka. Desain antar muka dapat dilihat pada gambar 2.Melalui perancangan yang telah dikerjakan, maka dapat diketahui diagram alir skematik dari penelitian ini (gambar 3). Pada diagram alir penelitian inidapat diketahuibahwa ketika prosestelahdimulai, hal yang dilakukukan terlebih dahuluialah menjalankanganache-cli. Kemudian, jalankantrufflecompile(Windows), lalu jalankan aplikasi Python. Jika tidak berhasil, maka coba jalankan kembali aplikasi Python. Jika aplikasi Python berhasil dijalankan, maka pengguna dapat melanjutkan dengan membuka controllerdan jalankan pin (on/off). Jika pin tidak berhasil dijalankan, maka buka kembali controlleratau lakukan refreshpada controller. Jika pin berhasil dijalankan, maka pada masing-masing terminal akan menampilkan riwayat transaksi yang berlangsung dan proses selesai.

HASIL DAN PEMBAHASAN

Untuk membuat program ini, kami menggunakan text editorVisual Studio Code serta menggunakan source codeyang terdapat pada akun Github SalmanDabbakuti(Dabbakuti, 2021), tetapi kami juga melakukan modifikasi pada controllerdengan menggunakan rancangan kami. Program yang telah dibuat, kemudian dijalankan padaprivate networkdan pengguna dapat melihat status setiap pin pada baris perintah dan juga padaemulator.Dimana pada dasarnya hasil akan menampilkan status pin tertentu pada blockchain dan kemudian mengaktifkan konfigurasi pin yang sesuai.

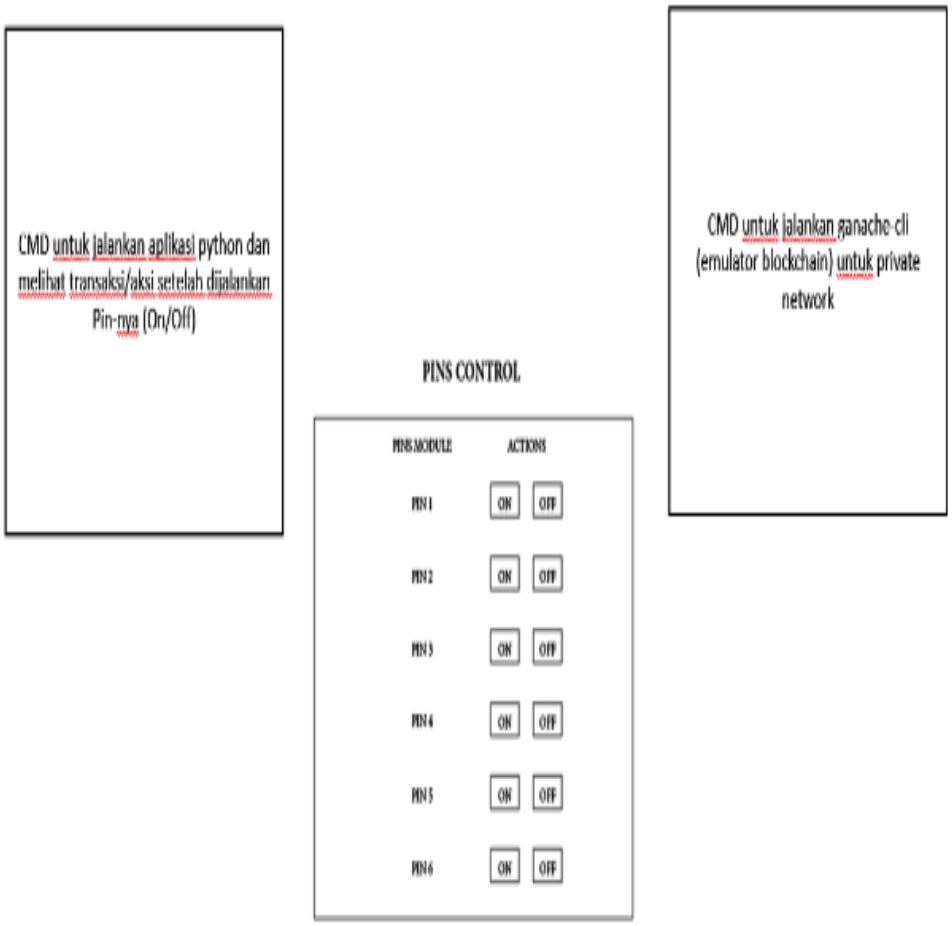
File Konfigurasi

Metadata konfigurasi mendefinisikan sebuah alur kerja tingkat tinggi dan model interaksi pada aplikasi blockchain. Untuk konfigurasi yang dilakukan terdapat pada file JSON (PatAltimore, 2022). Terdapat dua jenis file, yaitu home automationdan migrationspada penelitian kami.Peran konfigurasi yang dilakukan adalah untuk mendefinisikan tindakan yang terjadi dalam blockchain. Dalam hal ini akan terjadi skenario permintaan -tanggapan.

Hasil Demonstrasi

Programa.Instantiate ganache-cliprivate networkPada awal demonstrasi, hal pertama yang dilakukan oleh kami yaitu menjalankan ganache-cli private networkpada terminal (dalam hal ini kami menggunakan command promptpada sistem operasi Windows). Saat dijalankan maka akan menampilkan 10 akun yang tersedia dan 10 private keys yang dapat digunakan. Selain itu, pada terminal juga tertampil gas price, gas limit,call gas limit, dan juga itu berjalan pada port:8545.b. Compile contractSetelah menjalankan ganache-cli, selanjutnya jalankan truffle compile(untuk sistem operasi Windows) pada command prompt. Hal ini dilakukan untuk mengkompilasi contractyang ada pada direktori contractsdan membangun artefak pada direktori build

Gambar 1 Desain



Jalankan aplikasi Python

Kemudian, jalankan aplikasi Python yang tidak menggunakan private keyuntuk melakukan pengujian (public) pada private network. Setelah melakukan deployment contractspada private network, maka kita dapat melihat status setiap pin dibaris perintah dan pada emulator. Setelah aplikasi Python sudah dijalankan, maka transaksi akan mulai terhitung.d. Nyalakan atau matikan pinPengguna dapat melakukan turn onatauoffpin melalui controller. Pada simulasi ini, kami mencoba melakukan turn onpada pin 14 dan pin 18.

Penelitian ini membutuhkan sebuah skema pengiriman data yang mudah dimengerti atau dipahami, serta memerlukan data yang dapat dilaporkan dengan nilai hashpada data dantercatat pada jejaring blockchain.Pada bagian controller, perlu menambahkan fitur ketika button turning onatauoffdiklik,buttontersebut dapat berubah warna, sehingga pada controllerdapat terlihat lebih jelas pinyang dinyalakan atau dimatikan.

Pada penelitian ini memiliki metodologi yang belum cukup signifikan sehingga diperlukan penggabungan metodologi lainnya agar dapat menemukan kebaruan penelitian yang berbeda dengan penelitian lainnya. Selain itu, penelitian ini masih memiliki kekurangan untuk perhitungan dan analisis. Sehingga untuk penelitian selanjutnya, diharapkan dapat mengukur perbandingan maupun perhitungan dalam penggunaan blockchain di sebuah penelitian

KESIMPULAN DAN SARAN

Kesimpulan dari penelitian ini adalah implementasi blockchain pada perangkat IoT dapat meningkatkan keamanan data pada saat transaksi dilakukan karena sifatnya yang anonymous, tidak dapat melihat identitas asli pengguna dan data yang dikirim atau diterima tidak dapat diketahui oleh pihak lain karena data yang sudah dienkripsi menjadi sebuah kode dan hanya dapat diketahui oleh pengirim atau penerima saja. Sehingga data penting yang terdapat pada perangkat bisa terhindar dari berbagai ancaman yang dilakukan oleh pihak-pihak yang tidak diinginkan. Pada penelitian ini, implementasiblockchain berlangsung dengan menggunakan controlleruntuk mengontrol

semua pin yang terdapat pada emulator. Sehingga pada saat pin dinyalakan atau dimatikan akan menampilkan riwayat transaksi pada setiap terminal.

DAFTAR PUSTAKA

Ali , Ahmad. 2019. Blockchain based permission delegation and access control in Internet of Things (BACI). Computers & Security, 86, pp.318–334. https://doi.org/10.1016/j.cose.2019.06.010.

ATLAM, H. F., ALENEZI, A., ALASSAFI,M. O., & WILLS, G. B. (2018). Blockchain with Internet of Things: Benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications, 10(6), 40–48. https://doi.org/10.5815/ijisa.2018.06.05

BACCELLI, E., GUNDOGAN, C., HAHM, O., KIETZMANN, P., LENDERS, M. S., PETERSEN, H., SCHLEISER, K., SCHMIDT, T. C., & WAHLISCH, M. (2018). RIOT: An Open Source Operating System for Low-End Embedded Devices in the IoT. IEEE Internet of Things Journal, 5(6), 4428–4440. https://doi.org/10.1109/JIOT.2018.2815038

COLE, R., STEVENSON, M. &AITKEN, J., 2019. Blockchain technology: implications for operations and supply chain management. Supply Chain Management: An International Journal, 24(4),pp.469–483. https://doi.org/10.1108/SCM-09-2018-0309.DABBAKUTI, S., 2021. Salmandabbakuti/IoT-and-Blockchain. [Python] Available at: <https://github.com/Salmandabbakuti/IoT-and-Blockchain>

FADHILLAH, Y. et al. (2022). TEKNOLOGI BLOCKCHAIN DAN IMPLEMENTASINYA. Medan: Yayasan Kita MenulisFENG, B., MERA, A., & LU, L. (2020). P2IM: Scalable and Hardware-independent Firmware Testing via Automatic Peripheral Interface Modeling.https://www.usenix.org/conference/usenixsecurity20/presentation/feng

FERNANDO, E., MEYLIANA, H. &WARNARS, E.A., 2020. Blockchain technology for pharmaceutical drug distribution in Indonesia: A proposed model. ICIC Express Letters, 14(2), pp.113–120.

HELLIAR, C.V., CRAWFORD, L., ROCCA, L., TEODORI, C. &VENEZIANI, M., 2020. Permissionless and permissioned blockchain diffusion. International Journal of Information Management,54,p.102136. https://doi.org/10.1016/j.ijinfomgt.2020.102136.

HUANG, H., KONG, W., ZHOU, S., ZHENG, Z. &GUO, S., 2021. A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools. ACM Computing Surveys, 54(2), p.44:1-44:42. https://doi.org/10.1145/3441692

.KOSBA, A., MILLER, A., SHI, E., WEN, Z. &PAPAMANTHOU, C., 2016. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In: 2016 IEEE Symposium on Security and Privacy (SP). 2016 IEEE Symposium on Security and Privacy (SP). pp.839–858. https://doi.org/10.1109/SP.2016.55.

KOŠŤÁL, K., HELEBRANDT, P., BELLUŠ, M., RIES, M. &KOTULIAK, I., 2019. Management and Monitoring of IoT Devices Using Blockchain.Sensors,19(4),p.856. https://doi.org/10.3390/s19040856

.LOCKL, J., SCHLATT, V., SCHWEIZER, A., URBACH, N. &HARTH, N., 2020. Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications. IEEE Transactions on Engineering Management,67(4),pp.1256–1270. https://doi.org/10.1109/TEM.2020.2978014.

MATONDANG, N., NURLAILI ISNAINIYAH, I., & MULIAWATI, A. (2018). Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). 2(1), 282–287. http://jurnal.iaii.or.id

NAKAMOTO, S., 2008. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, p.21260.PANARELLO, A., TAPAS, N., MERLINO, G., LONGO, F. &PULIAFITO, A., 2018. Blockchain and IoT Integration: A Systematic Survey.Sensors,18(8),p.2575. https://doi.org/10.3390/s18082575.PATALTIMORE, 2022. Create a blockchain application -Azure Blockchain Workbench -Azure Blockchain.

PRAMUDITA, R., FUADA, S., & MAJID, N. W. A. (2020). Studi Pustaka Tentang Kerentanan Keamanan E-Learning dan Penanganannya. JURNAL MEDIA INFORMATIKA BUDIDARMA, 4(2), 309. https://doi.org/10.30865/mib.v4i2.1934

PURI, V., PRIYADARSHINI, I., KUMAR, R., & VAN LE, C. (2021). Smart contract based policies for the Internet of Things. Cluster Computing, 24(3), 1675–1694. https://doi.org/10.1007/s10586-020-03216-w

RIADI, I., UMAR, R. &LESTARI, T., 2021. Smart Payment Application Security Optimization from Cross-Site Scripting (XSS) Attacks Based on Blockchain Technology. Telematika,14(2), pp.74–85. https://doi.org/10.35671/telematika.v14i2.1221.

SARI, I.Y. et al. (2020). KEAMANAN DATA DAN INFORMASI.Medan: Yayasan Kita MenulisSIDIQ, M.F., BASUKI, A.I., FIRDAUS, H. &BAIHAQI, M.A., 2020. Sentralisasi Pengawasan Informasi Jaringan Menggunakan Blockchain Ethereum. Jurnal Teknologi Informasi dan Ilmu Komputer,7(6),pp.1187–1196. https://doi.org/10.25126/jtiik.2020722662.

ZHOU, L., WANG, L., SUN, Y., & LV, P. (2018). BeeKeeper: A Blockchain-Based IoT System with Secure Storage and Homomorphic Computation. IEEE Access, 6, 43472–43488. https://doi.org/10.1109/ACCESS.2018.2847632