JUTECH
Journal Education and Technology
http://jurnal.stkippersada.ac.id/jurnal/index.php/jutech/index
E - ISSN 2722-9297
APTIKOM

PENGAMANAN DATA SENSOR IOT DENGAN TEKNOLOGI *BLOCKCHAIN* UNTUK *SMART HOME*

Rido Ramadhani[1], Herwis Gultom[2], Irgi Fahreza Ramadhan[3], Shifany Salsabila[4,] Oki Herdiyanto[5]
[1,2,3,4,5] *Teknik Informatika, Universitas Pamulang*
email: ridoramadhani29@gmail.com[1], dosen02535@unpam.ac.id [2], irgifahrezaramadhan@gmail.com[3], shifani22salsabila@gmail.com[4,] okkyherdianto1@gmail.com[5]

Informasi Artikel

Riwayat artikel :
Disubmit : 30 November 2024
Direvisi : 3 Desember 2024
Diterima : 5 Desember 2024
Dipublikasi : 20 Desember 2024

Keywords:
IoT, Blockchain, Data Security, Smart Home, Sensor, Smart Contract, Cryptography, Privacy, Security System, Internet of Things.

ABSTRACT

Internet of Things (IoT) technology brings convenience to smart home deployments, but presents significant challenges such as data security, energy efficiency, and resilience to cyberattacks such as Denial of Service (DoS). IoT data is often vulnerable to manipulation, while the power limitations of devices are an obstacle to stable and efficient operation. In addition, the centralised architecture of IoT is vulnerable to attacks, which can cause serious operational disruptions. This research aims to address these challenges by implementing blockchain technology using the Proof of Stake (PoS) consensus algorithm. An experimental approach is used to evaluate data security, energy consumption, and network resilience to DoS attacks on simulated IoT devices. The results show that blockchain is able to protect data integrity through hashing, maintain low energy consumption of 0.02 kWh per transaction, and remain stable despite up to 10,000 fake requests per minute. These findings show that blockchain improves not only data security but also energy efficiency and threat resistance, making it an ideal solution for smart home development. In conclusion, the application of blockchain offers a secure, efficient, and reliable foundation for the IoT ecosystem, making a significant contribution to future smart home technology innovation.

Kata Kunci: :
IoT, *Blockchain*, Keamanan Data, *Smart Home*, Sensor, *Smart Contract*, Kriptografi, Privasi, Sistem Pengamanan, Internet of Things.

ABSTRAK

Teknologi Internet of Things (IoT) memberikan kemudahan pada penerapan rumah pintar (*smart home*), tetapi menghadirkan tantangan signifikan seperti keamanan data, efisiensi energi, dan ketahanan terhadap serangan siber seperti *Denial of Service (DoS)*. Data IoT sering rentan terhadap manipulasi, sementara keterbatasan daya perangkat menjadi kendala untuk operasi yang stabil dan efisien. Selain itu, arsitektur terpusat IoT rentan terhadap serangan, yang dapat menyebabkan gangguan operasional serius. Penelitian ini bertujuan untuk mengatasi tantangan tersebut dengan menerapkan teknologi *blockchain* menggunakan algoritma konsensus *Proof of Stake (PoS)*. Pendekatan eksperimen digunakan untuk mengevaluasi keamanan data, konsumsi energi, dan ketahanan jaringan terhadap serangan DoS pada perangkat IoT simulasi. Hasil penelitian menunjukkan bahwa *blockchain* mampu melindungi integritas data melalui hashing, menjaga konsumsi energi rendah sebesar 0,02 kWh per transaksi, dan tetap stabil meskipun terdapat hingga 10.000 permintaan palsu per menit. Temuan ini menunjukkan bahwa *blockchain* tidak hanya meningkatkan keamanan data tetapi juga efisiensi energi dan ketahanan terhadap ancaman, menjadikannya solusi ideal untuk pengembangan rumah pintar. Kesimpulannya, penerapan *blockchain* menawarkan fondasi yang aman, efisien, dan andal bagi ekosistem IoT, memberikan kontribusi signifikan bagi inovasi teknologi rumah pintar masa depan.

JUTECH
Journal Education and Technology
http://jurnal.stkippersada.ac.id/jurnal/index.php/jutech/index
E - ISSN 2722-9297
APTIKOM

PENDAHULUAN

Perkembangan teknologi *Internet of Things (IoT)* telah mengubah cara manusia berinteraksi dengan lingkungan, menciptakan ekosistem di mana perangkat elektronik dapat saling terhubung dan berkomunikasi secara otomatis. IoT memainkan peran penting dalam membangun konsep rumah pintar (*smart home*), yang dirancang untuk meningkatkan kenyamanan, efisiensi, dan keamanan pengguna. Sistem rumah pintar memungkinkan kontrol otomatis pada perangkat seperti pencahayaan, pendingin ruangan, pengamanan, dan perangkat elektronik lainnya melalui jaringan internet. Namun, terlepas dari kemajuannya, adopsi IoT masih menghadapi tantangan mendasar, yaitu masalah keamanan data, konsumsi energi, dan ketahanan terhadap serangan siber (Cahyono & Hadikurniawati, 2023)

Persoalan keamanan menjadi perhatian utama dalam IoT. Data yang dikirimkan antar perangkat sering kali berisi informasi sensitif seperti pola aktivitas pengguna dan data pribadi lainnya. Ketidakamanan jaringan dapat menyebabkan data ini menjadi target serangan siber seperti *man-in-the-middle* atau penyadapan data. Selain itu, perangkat IoT umumnya memiliki sumber daya yang terbatas, seperti daya baterai dan kapasitas pemrosesan, sehingga sulit untuk menerapkan protokol keamanan yang kompleks (Prawiyogi & Anwar, 2023). Kekurangan ini diperparah oleh sifat arsitektur IoT yang terpusat, di mana satu titik kegagalan dapat menyebabkan gangguan signifikan dalam sistem secara keseluruhan (Wihartiko et al., 2021)

Tantangan lain adalah efisiensi energi. Sebagian besar perangkat IoT bergantung pada sumber daya terbatas, sehingga sistem keamanan yang efisien dalam penggunaan daya sangat dibutuhkan. Penggunaan algoritma tradisional pada sistem IoT seringkali meningkatkan konsumsi energi, yang tidak sesuai untuk perangkat bersumber daya rendah seperti sensor dan aktuator. Selain itu, serangan siber seperti *Denial of Service* (DoS) dapat mengganggu sistem dengan mengirimkan ribuan permintaan palsu, yang dapat meningkatkan beban pemrosesan dan menguras energi perangkat (Perdani et al., 2018).

Blockchain muncul sebagai solusi potensial untuk mengatasi berbagai persoalan ini. Sebagai teknologi desentralisasi, *blockchain* memungkinkan data disimpan secara terdistribusi sehingga mengurangi risiko serangan pada satu titik kegagalan. Algoritma konsensus seperti *Proof of Stake* (PoS) juga menawarkan efisiensi energi yang signifikan dibandingkan metode tradisional seperti *Proof of Work* (PoW(Prawiyogi & Anwar, 2023) Selain itu, *blockchain* dilengkapi dengan mekanisme hashing kriptografi yang melindungi data dari manipulasi, serta memastikan bahwa hanya entitas yang diotorisasi yang dapat mengakses informasi(Anhar & Pratama, 2024).

Dalam konteks rumah pintar, *blockchain* tidak hanya berperan dalam meningkatkan keamanan data, tetapi juga memberikan efisiensi energi yang signifikan. Kombinasi IoT dengan *blockchain*

JUTECH
Journal Education and Technology
http://jurnal.stkippersada.ac.id/jurnal/index.php/jutech/index
E - ISSN 2722-9297

menawarkan peluang baru untuk menciptakan ekosistem rumah pintar yang lebih aman, efisien, dan andal. Oleh karena itu, penelitian ini berfokus pada penerapan *blockchain* untuk meningkatkan keamanan, efisiensi energi, dan ketahanan terhadap serangan siber dalam sistem rumah pintar berbasis IoT. Penelitian ini diharapkan memberikan kontribusi signifikan terhadap pengembangan teknologi IoT yang lebih matang dan aman.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian eksperimental berbasis pengembangan sistem dengan pendekatan kuantitatif. Tahapan penelitian meliputi:

1. Analisis Kebutuhan

   Pada tahap ini, dilakukan identifikasi kebutuhan keamanan data pada ekosistem IoT rumah pintar. Analisis dilakukan melalui studi literatur untuk memahami celah keamanan data sensor IoT dan potensi penerapan teknologi *blockchain*(Le Nguyen et al., 2020).

2. Perancangan Sistem

   Dirancang arsitektur sistem yang mengintegrasikan teknologi *blockchain* dengan perangkat IoT. Desain mencakup alur penyimpanan data sensor pada *blockchain*, pengelolaan autentikasi melalui *smart contract,* dan penggunaan algoritma kriptografi kunci publik untuk menjaga privasi data(Sharma et al., 2018).

3. Pengembangan Prototipe

   Prototipe sistem dibangun menggunakan platform *blockchain* publik, seperti *Ethereum* atau *Hyperledger Fabric*. Data sensor IoT disimulasikan menggunakan perangkat lunak untuk menguji interoperabilitas antara perangkat IoT dan *blockchain*(Zhang & Wen, 2017).

4. Pengujian dan Evaluasi

   Prototipe diuji untuk mengevaluasi kinerja sistem dari segi:

   a. Keamanan: Mengukur tingkat integritas data menggunakan uji serangan simulasi (*penetration testing*).
   b. Efisiensi: Menilai waktu transaksi, latensi, dan konsumsi daya pada perangkat IoT yang terhubung ke *blockchain*.
   c. Keandalan: Menganalisis ketahanan sistem terhadap kegagalan dan upaya akses tidak sah.

5. Analisis Data

   Data hasil pengujian dianalisis secara kuantitatif menggunakan statistik deskriptif untuk memahami pola performa dan efektivitas sistem.

JUTECH
Journal Education and Technology
http://jurnal.stkippersada.ac.id/jurnal/index.php/jutech/index
E - ISSN 2722-9297
APTIKOM

6. Penyimpulan

Hasil analisis digunakan untuk menyimpulkan keefektifan pendekatan *blockchain* dalam pengamanan data sensor IoT, sekaligus mendokumentasikan pengembangan sistem untuk digunakan dalam penelitian lanjutan.

HASIL DAN PEMBAHASAN

Hasil Penelitian

1. Keamanan Data

Penelitian ini berhasil menguji kemampuan *blockchain* dalam menjaga integritas data sensor IoT dari berbagai ancaman keamanan, seperti manipulasi data dan serangan *Man-in-the-Middle (MITM)*. Hasil menunjukkan bahwa semua upaya manipulasi data gagal karena *blockchain* memanfaatkan algoritma hashing yang mengamankan setiap blok data. Jika terjadi perubahan pada data, hash blok tidak akan cocok dengan blok berikutnya, sehingga sistem dapat mendeteksi manipulasi.

Tabel 1. Hasil Pengujian Keamanan Data Sensor IoT

Jenis Serangan	Target	Hasil	Keterangan
Man-in-the-Middle (MITM)	Sensor ke *Blockchain*	Tidak berhasil	Data tetap utuh tanpa modifikasi
Manipulasi Data	Block dalam *Blockchain*	Tidak berhasil	Hash blok mendeteksi perubahan data

2. Efisiensi Transaksi

Waktu transaksi untuk menyimpan data sensor diuji menggunakan platform *blockchain* publik. Pengujian dilakukan pada lima skenario dengan jumlah data yang berbeda untuk mengukur efisiensi waktu transaksi.

Tabel 2. Rata-rata Waktu Transaksi Berdasarkan Ukuran Data

Ukuran Data (*byte*)	Waktu Transaksi (detik)	Status Efisiensi
100	3,1	Sangat Efisien
500	3,4	Stabil
1.000	3,5	Stabil
5.000	4,5	Mulai lambat
10.000	5,2	Sedikit melambat

JUTECH
Journal Education and Technology
http://jurnal.stkippersada.ac.id/jurnal/index.php/jutech/index
E - ISSN 2722-9297
APTIKOM

3. Konsumsi Energi

Salah satu tantangan dalam sistem IoT adalah efisiensi energi. Penelitian ini mengukur konsumsi energi rata-rata setiap transaksi. Hasil menunjukkan bahwa rata-rata energi yang digunakan adalah 0,02 kWh per transaksi, dengan nilai tertinggi hanya 0,023 kWh.

Tabel 3. Konsumsi Energi Berdasarkan Jumlah Transaksi

Jumlah Transaksi	Energi Total (kWh)	Rata-rata Energi/Transaksi (kWh)
10	0,2	0,02
50	1,1	0,022
100	2,3	0,023

4. Ketahanan terhadap Serangan DoS

Penelitian ini juga menguji ketahanan sistem terhadap serangan *Denial of Service (DoS)* dengan mengirimkan hingga 10.000 permintaan palsu per menit. Hasil menunjukkan bahwa sistem tetap stabil dan dapat menolak permintaan palsu tanpa mengganggu proses transaksi yang sah.

Tabel 4. Ketahanan Sistem terhadap Serangan DoS

Jumlah Permintaan Palsu (per menit)	Status Sistem	Keterangan
1.000	Stabil	Tidak ada pengaruh signifikan
5.000	Stabil	Respon tetap lancer
10.000	Stabil	Tidak ada gangguan transaksi sah

Pembahasan Penelitian

1. Keamanan Data

Keamanan data merupakan elemen fundamental dalam sistem IoT, khususnya untuk rumah pintar, karena perangkat IoT sering kali bekerja di lingkungan terbuka yang rentan terhadap ancaman keamanan, seperti pencurian data, manipulasi data, dan serangan *Man-in-the-Middle (MITM)*. Penelitian ini menunjukkan bahwa *blockchain*, dengan arsitektur desentralisasi dan mekanisme hashing, mampu memberikan perlindungan yang kuat terhadap ancaman tersebut.

Mekanisme hashing *blockchain* memastikan bahwa setiap perubahan kecil dalam blok data akan mengakibatkan seluruh rantai data tidak sesuai, sehingga mudah terdeteksi. Dalam simulasi serangan MITM yang dilakukan selama penelitian, data sensor IoT yang diubah oleh pihak tidak sah langsung terdeteksi sebagai tidak valid oleh sistem *blockchain*. Hal ini

JUTECH
Journal Education and Technology
http://jurnal.stkippersada.ac.id/jurnal/index.php/jutech/index
E - ISSN 2722-9297
APTIKOM

disebabkan oleh sifat kriptografis *blockchain*, di mana setiap blok data memiliki sidik jari digital (*digital fingerprint*) yang saling terkait. Dengan demikian, *blockchain* secara efektif meminimalkan risiko manipulasi data.

Penerapan algoritma konsensus *Proof of Stake (PoS)* semakin meningkatkan keamanan, karena hanya node-node terpercaya yang dapat memvalidasi transaksi. Berbeda dengan pendekatan tradisional seperti *Proof of Work (PoW)* yang membutuhkan proses komputasi intensif, PoS mengurangi risiko sentralisasi daya komputasi yang dapat dieksploitasi oleh pihak tidak sah. Hal ini menjadikan *blockchain* lebih aman dan efisien untuk diterapkan pada sistem rumah pintar(Guan et al., 2021).

Tabel 5. Keamanan Data

Ancaman	**Mekanisme Perlindungan *Blockchain***	**Hasil**
Manipulasi Data	Hashing	Tidak ada data yang berubah
Serangan MITM	Validasi oleh node terpercaya (PoS)	Transaksi tidak terganggu
Pengaksesan data tidak sah	Enkripsi data	Data tetap aman

2. Efisiensi Transaksi

Sistem rumah pintar sering kali memerlukan respon *real-time* untuk memastikan fungsionalitas yang optimal, seperti membuka pintu secara otomatis, menyalakan lampu berdasarkan kehadiran pengguna, atau mengatur suhu ruangan. Waktu rata-rata transaksi *blockchain* sebesar 3,5 detik untuk data berukuran 1.000 byte menunjukkan bahwa teknologi ini dapat memproses data dengan cepat, memenuhi kebutuhan operasional IoT rumah pintar (Parung et al., 2021).

Penelitian ini juga menunjukkan stabilitas waktu pemrosesan untuk berbagai ukuran data. Pada data kecil hingga menengah (100 hingga 10.000 byte), waktu transaksi tidak mengalami peningkatan signifikan. Hal ini mencerminkan efisiensi *blockchain* dalam mengelola data yang umumnya dihasilkan oleh perangkat IoT, seperti sensor suhu, kamera, atau perangkat keamanan (Prawiyogi & Anwar, 2023).

JUTECH
Journal Education and Technology
http://jurnal.stkippersada.ac.id/jurnal/index.php/jutech/index
E - ISSN 2722-9297

Tabel 6. Waktu Transaksi untuk Berbagai Ukuran Data

Ukuran Data *(byte)*	Waktu Transaksi (detik)
100	3,1
1.000	3,5
10.000	4.0

Efisiensi ini dicapai melalui penggunaan algoritma PoS, di mana proses validasi dilakukan oleh node yang dipilih berdasarkan kepemilikan token, bukan berdasarkan kemampuan komputasi. Pendekatan ini tidak hanya meningkatkan kecepatan transaksi tetapi juga mengurangi beban jaringan, menjadikan sistem lebih responsif dan stabil (Simanungkalit, 2024).

3. Konsumsi Energi

Salah satu tantangan utama dalam implementasi IoT di rumah pintar adalah keterbatasan energi pada perangkat IoT, yang sering menggunakan sumber daya terbatas seperti baterai atau energi terbarukan. Oleh karena itu, efisiensi energi menjadi salah satu aspek yang sangat penting dalam mengintegrasikan teknologi baru seperti *blockchain*. Penelitian ini menunjukkan bahwa dengan menggunakan algoritma konsensus *Proof of Stake (PoS)*, *blockchain* dapat mengurangi konsumsi energi secara signifikan dibandingkan dengan algoritma *Proof of Work (PoW)*, yang sering digunakan dalam sistem *blockchain* tradisional (Sumampouw & Sembiring, 2024).

Penelitian ini mengukur konsumsi energi *blockchain* untuk transaksi yang dilakukan pada data IoT. Konsumsi energi rata-rata tercatat sekitar 0,02 kWh per transaksi, yang sangat rendah, terutama jika dibandingkan dengan konsumsi energi yang dibutuhkan untuk proses mining dalam algoritma PoW. Dengan angka ini, sistem *blockchain* dapat diterapkan pada perangkat IoT yang memiliki keterbatasan daya, seperti sensor suhu, kamera keamanan, atau perangkat pengendalian otomatis lainnya, tanpa membebani sumber daya perangkat.

Perangkat IoT rumah pintar, yang sering kali menggunakan baterai kecil atau sumber daya terbarukan, memerlukan sistem yang hemat energi. Konsumsi energi *blockchain* yang rendah ini sangat mendukung keberlanjutan sistem rumah pintar, mengingat perangkat IoT beroperasi sepanjang waktu dan membutuhkan penggunaan sumber daya yang efisien (Prawiyogi & Anwar, 2023).

Tabel 7. Konsumsi Energi *Blockchain*

Parameter	Nilai
Konsumsi Energi	0,02 kWh/transaksi
Kapasitas Baterai IoT	4,0 kWh
Operasional Maksimum	>200 Transaksi

JUTECH
Journal Education and Technology
http://jurnal.stkippersada.ac.id/jurnal/index.php/jutech/index
E - ISSN 2722-9297
APTIKOM

Dari tabel di atas, dapat disimpulkan bahwa dengan kapasitas baterai sebesar 4 kWh, sistem dapat menangani lebih dari 200 transaksi *blockchain* per perangkat IoT tanpa mengalami masalah daya. Hal ini memperlihatkan bagaimana *blockchain* dengan PoS bisa menjadi solusi efisien dalam menjaga kelangsungan operasi IoT rumah pintar tanpa mengorbankan efisiensi energi.

4. Ketahanan terhadap Serangan DoS

Salah satu ancaman utama bagi sistem IoT adalah serangan *Denial of Service (DoS)*, yang berpotensi mengganggu operasi normal dengan membanjiri sistem dengan permintaan palsu atau berlebihan. Dalam rumah pintar, serangan DoS dapat mengganggu berbagai layanan penting, seperti pengendalian suhu atau penguncian pintu otomatis. Penelitian ini menguji ketahanan sistem *blockchain* terhadap serangan DoS untuk memastikan bahwa sistem dapat bertahan dalam kondisi jaringan yang penuh tekanan.

Blockchain, yang beroperasi dalam arsitektur desentralisasi, terbukti lebih tahan terhadap serangan DoS dibandingkan dengan sistem terpusat. Setiap transaksi pada *blockchain* divalidasi oleh node-node yang tersebar dalam jaringan, yang berarti serangan terhadap satu atau beberapa node tidak akan mempengaruhi keseluruhan sistem. Dalam penelitian ini, simulasi dilakukan untuk mensimulasikan 10.000 permintaan palsu per menit, dan sistem *blockchain* tetap stabil tanpa adanya gangguan berarti pada transaksi sah (Abdullah, 2023).

Tabel 8. Waktu Transaksi untuk Berbagai Ukuran Data

Jumlah Permintaan Palsu	Status Jaringan
1.000	Stabil
5.000	Stabil
10.000	Stabil

Penjelasan:

Jumlah permintaan palsu yang semakin banyak diuji untuk melihat apakah *blockchain* dapat mengatasi beban yang meningkat.

Status jaringan tetap stabil meskipun jumlah permintaan palsu meningkat, menunjukkan bahwa *blockchain* dapat mengelola lalu lintas jaringan tinggi yang terjadi pada IoT rumah pintar dengan baik.

Hasil ini menunjukkan bahwa *blockchain* dapat mengatasi gangguan dari serangan DoS tanpa mengganggu operasi transaksi sah, memastikan bahwa rumah pintar tetap aman dan

JUTECH
Journal Education and Technology
http://jurnal.stkippersada.ac.id/jurnal/index.php/jutech/index
E - ISSN 2722-9297
APTIKOM

fungsional, meskipun terpapar ancaman eksternal. Hal ini memberikan keunggulan bagi penerapan IoT rumah pintar berbasis *blockchain*, yang harus tetap andal dalam berbagai kondisi(Swasono & Muthmainah, 2023).

5. Relevansi *Blockchain* untuk IoT Rumah Pintar

Temuan dari penelitian ini memperlihatkan bahwa *blockchain* dapat menjadi solusi komprehensif yang sangat relevan untuk mendukung keamanan, efisiensi, dan ketahanan sistem IoT di rumah pintar. Keamanan data, efisiensi energi, dan ketahanan terhadap serangan DoS adalah tiga aspek utama yang menjadi fokus dalam penelitian ini. Hasil yang diperoleh menunjukkan bahwa *blockchain* dengan algoritma konsensus PoS dapat mengatasi tantangan-tantangan tersebut dengan sangat efektif. *Blockchain* memberikan perlindungan data melalui mekanisme kriptografi dan integritas transaksi yang kuat. Selain itu, efisiensi energi yang tinggi dan konsumsi daya rendah menjadikan teknologi ini sangat cocok untuk diterapkan dalam perangkat IoT yang memiliki sumber daya terbatas. Ketahanan terhadap serangan DoS juga memberikan keamanan yang lebih terhadap potensi gangguan dari luar(Dorri et al., 2017).

Secara keseluruhan, hasil penelitian ini mendukung penerapan *blockchain* untuk IoT rumah pintar, tidak hanya untuk meningkatkan keamanan data tetapi juga untuk memastikan sistem berjalan dengan lancar dan dapat diandalkan. Dengan mengatasi isu-isu seperti penggunaan energi yang tinggi dan potensi gangguan jaringan, *blockchain* membuka peluang untuk menciptakan ekosistem rumah pintar yang lebih aman, efisien, dan tahan lama(Prawiyogi & Anwar, 2023b).

SIMPULAN

Penelitian ini berhasil mengungkapkan potensi besar teknologi *blockchain* dalam meningkatkan keamanan, efisiensi energi, dan ketahanan terhadap serangan dalam penerapan *Internet of Things (IoT)* pada sistem rumah pintar. Berdasarkan hasil pengujian yang dilakukan, *blockchain* dengan algoritma konsensus *Proof of Stake (PoS)* terbukti memberikan solusi yang efisien dalam hal konsumsi energi, di mana konsumsi rata-rata tercatat hanya sebesar 0,02 kWh per transaksi. Hal ini menunjukkan bahwa *blockchain* dapat diterapkan pada perangkat IoT yang memiliki keterbatasan daya, seperti sensor suhu, pengendali pintu otomatis, dan perangkat lainnya yang menggunakan baterai atau sumber energi terbarukan. Selain itu, *blockchain* juga terbukti memiliki ketahanan yang kuat terhadap serangan *Denial of Service (DoS)*, dengan mampu menangani hingga 10.000 permintaan palsu per menit tanpa mengganggu integritas dan kestabilan sistem. Hasil tersebut mengkonfirmasi bahwa *blockchain*, yang bekerja dalam sistem desentralisasi, menawarkan keamanan data yang lebih kuat dan memastikan

JUTECH
Journal Education and Technology
http://jurnal.stkippersada.ac.id/jurnal/index.php/jutech/index
E - ISSN 2722-9297
APTIKOM

bahwa operasional rumah pintar dapat berjalan lancar meskipun terpapar ancaman dari luar (Ilhami, 2022).

Penelitian ini juga menunjukkan bahwa *blockchain* bukan hanya meningkatkan keamanan data melalui mekanisme kriptografi, tetapi juga memungkinkan transaksi yang lebih efisien dan cepat tanpa mengorbankan daya. Teknologi ini dapat menjadi fondasi bagi pengembangan sistem rumah pintar yang lebih aman, efisien, dan tahan lama, serta lebih hemat energi. Dengan berbagai keunggulannya, *blockchain* dapat mengatasi tantangan utama yang sering dihadapi dalam integrasi IoT, seperti perlindungan data sensitif, efisiensi penggunaan energi, dan ketahanan terhadap gangguan eksternal. Oleh karena itu, penerapan *blockchain* pada IoT rumah pintar memiliki potensi besar untuk menciptakan ekosistem yang lebih aman dan berkelanjutan. Penelitian ini berkontribusi pada pengembangan teknologi IoT dan *blockchain*, membuka peluang untuk penerapan lebih luas dalam berbagai sektor lain yang memerlukan keamanan dan efisiensi tinggi, terutama di era smart cities yang sedang berkembang pesat.

DAFTAR RUJUKAN

Abdullah, N. R. (2023). IMPLEMENTASI TEKNOLOGI *BLOCKCHAIN* DALAM KEAMANAN SISTEM KOMPUTER TERDISTRIBUSI. *Jurnal Teknologi Terkini*, *3*(7).

Anhar, M. A., & Pratama, T. A. (2024). Analisis Implementasi Keamanan Data melalui Teknologi *Blockchain* (Studi Kasus Pustipada UINSU). *Jurnal Ilmu Komputer (JUIK)*, *4*(2), 58–67.

Cahyono, T. D., & Hadikurniawati, W. (2023). *BLOCKCHAIN* UNTUK APLIKASI IOT HEALTHCARE: STUDI LITERATUR. *Dinamik*, *28*(2), 53–60.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). *Blockchain* for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634

Guan, Z., Lu, X., Yang, W., Wu, L., Wang, N., & Zhang, Z. (2021). Achieving efficient and Privacy-preserving energy trading based on *blockchain* and ABE in smart grid. *Journal of Parallel and Distributed Computing*, *147*, 34–45. https://doi.org/10.1016/j.jpdc.2020.08.012

Ilhami, D. A. S. (2022). Data privasi dan keamanan siber pada smart-city: Tinjauan literatur. *Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi*, *2*(1), 51–60.

Le Nguyen, B., Lydia, E. L., Elhoseny, M., Pustokhina, I., Pustokhin, D. A., Selim, M. M., Nguyen, G. N., & Shankar, K. (2020). Privacy preserving *blockchain* technique to achieve secure and reliable sharing of IoT data. *Computers, Materials & Continua*, *65*(1), 87–107.

JUTECH
Journal Education and Technology
http://jurnal.stkippersada.ac.id/jurnal/index.php/jutech/index
E - ISSN 2722-9297
APTIKOM

Parung, J., Larissa, S., Santoso, A., & Prayogo, D. N. (2021). *Penggunaan Teknologi Blokchain, Internet Of Things Dan Artifial Intelligence Untuk Mendukung Kota Cerdas. Studi Kasus: Supply Chain Industri Perikanan*. Universitas Surabaya.

Perdani, M. D. K., Widyawan, W., & Santosa, P. I. (2018). *Blockchain* untuk Keamanan Transaksi Elektronik Perusahaan Financial Technology (Studi Kasus pada PT XYZ). *Semnasteknomedia Online*, *6*(1), 1–14.

Prawiyogi, A. G., & Anwar, A. S. (2023b). Perkembangan Internet of Things (IoT) pada Sektor Energi: Sistematik Literatur Review. *Jurnal MENTARI: Manajemen, Pendidikan Dan Teknologi Informasi*, *1*(2), 187–197.

Sharma, P. K., Kumar, N., & Park, J. H. (2018). *Blockchain*-based distributed framework for automotive industry in a smart city. *IEEE Transactions on Industrial Informatics*, *15*(7), 4197–4205.

Simanungkalit, A. (2024). Teknologi *Blockchain*: Solusi untuk Keamanan Data dalam Transaksi Digital. *Circle Archive*, *1*(6).

Sumampouw, E. G. J., & Sembiring, I. (2024). Analisis Verifikasi Proof of Stake (POS) NFT dengan Teknologi Smart Contract. *Edutik: Jurnal Pendidikan Teknologi Informasi Dan Komunikasi*, *4*(1), 15–28.

Swasono, M. A. H., & Muthmainah, H. N. (2023). Pemanfaatan Teknologi Informasi dalam Optimalisasi Produksi Tanaman Pangan: Studi Bibliometrik Skala Nasional. *Jurnal Multidisiplin West Science*, *2*(08), 668–683.

Wihartiko, F. D., Nurdiati, S., Buono, A., & Santosa, E. (2021). *Blockchain* dan kecerdasan buatan dalam pertanian: studi literatur. *J. Teknol. Inf. Dan Ilmu Komput*, *8*(1), 177.

Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using *blockchain* technology for the internet of things. *Peer-to-Peer Networking and Applications*, *10*(4), 983–994. https://doi.org/10.1007/s12083-016-0456-1