

DESENTRALISASI SISTEM KEAMANAN IOT RUMAH PINTAR BERBASIS BLOCKCHAIN

Ardilla Ekrinifda, Agus Wiranto

Teknik Informatika, Universitas Pamulang

Jl. Raya Puspitek, Buaran, Kec. Pamulang, Kota Tangerang Selatan, Banten, Indonesia

ardillaekrinifda2@gmail.com

ABSTRAK

Perkembangan Internet of Things (IoT) mendorong penerapan sistem rumah pintar, khususnya pada perangkat keamanan seperti Closed Circuit Television (CCTV). Namun, sistem penyimpanan rekaman CCTV yang masih bersifat terpusat memiliki kelemahan berupa risiko kehilangan data, manipulasi, serta ketergantungan pada satu media penyimpanan. Permasalahan tersebut berpotensi mengurangi keandalan sistem keamanan rumah pintar. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan IoT rumah pintar berbasis blockchain dengan memanfaatkan InterPlanetary File System (IPFS) sebagai media penyimpanan terdistribusi guna meningkatkan keamanan, integritas, dan ketersediaan data rekaman CCTV. Metode penelitian yang digunakan adalah metode prototipe, yang meliputi proses perekaman CCTV, penyimpanan video ke IPFS untuk menghasilkan Content Identifier (CID), serta pencatatan CID ke dalam blockchain melalui smart contract pada jaringan blockchain privat. Pengujian dilakukan pada aspek distribusi data, integritas data, dan ketersediaan data. Hasil penelitian menunjukkan bahwa rekaman CCTV berhasil disimpan secara terdesentralisasi, perubahan data dapat terdeteksi melalui perbedaan CID, serta data tetap dapat diakses meskipun terjadi gangguan pada penyimpanan lokal. Dengan demikian, integrasi blockchain dan IPFS terbukti efektif sebagai solusi alternatif penyimpanan rekaman CCTV pada sistem rumah pintar.

Kata kunci: *Internet of Things; SmartHome; CCTV; Blockchain; IPFS*

1. PENDAHULUAN

Pada sistem CCTV yang beredar di pasaran saat ini, proses penyimpanan data rekaman umumnya masih bergantung pada Digital Video Recorder (DVR) atau media penyimpanan lokal dan terpusat lainnya, seperti hard disk internal atau penyimpanan berbasis cloud milik penyedia layanan tertentu. Model penyimpanan terpusat tersebut memiliki kelemahan signifikan, terutama terkait keamanan dan ketersediaan data rekaman video[1].

Dalam praktiknya, data rekaman CCTV sering kali mengalami kehilangan, baik akibat kerusakan perangkat penyimpanan, kegagalan sistem, serangan siber, maupun tindakan penghapusan yang disengaja oleh pihak yang tidak bertanggung jawab. Kondisi ini menjadi permasalahan serius, mengingat rekaman CCTV memiliki nilai penting sebagai bukti keamanan, dokumentasi kejadian, serta alat pendukung investigasi. Hilangnya data rekaman tersebut dapat mengakibatkan terhambatnya proses penelusuran kejadian dan menurunkan tingkat kepercayaan terhadap sistem keamanan rumah pintar.

Berdasarkan permasalahan tersebut, diperlukan suatu pendekatan alternatif yang mampu menjamin ketersediaan, integritas, dan ketahanan data rekaman CCTV terhadap manipulasi maupun penghapusan sepihak. Teknologi blockchain menawarkan karakteristik desentralisasi dan sifat immutable, di mana data yang telah dicatat tidak dapat diubah atau dihapus tanpa terdeteksi. Dengan menggabungkan blockchain dan sistem penyimpanan terdistribusi

seperti InterPlanetary File System (IPFS), data rekaman CCTV dapat disimpan secara terdesentralisasi tanpa bergantung pada satu titik penyimpanan[3].

Beberapa penelitian sebelumnya telah mengkaji pemanfaatan teknologi blockchain dan sistem penyimpanan terdistribusi. Pada penelitian yang dikaji oleh (Irawan & Trihatmojo, 2024) yang berjudul *Decentralized Trusted Storage of Audio-Video Log Data Based on Blockchain Technology and IPFS* mengusulkan sistem penyimpanan log audio dan video secara terdesentralisasi dengan memanfaatkan teknologi blockchain dan InterPlanetary File System (IPFS)[4]. Data multimedia disimpan pada jaringan IPFS, sedangkan nilai hash data dicatat pada blockchain untuk menjamin integritas dan ketertelusuran data. Hasil penelitian menunjukkan bahwa sistem ini mampu mencegah manipulasi dan penghapusan data secara sepihak, serta meningkatkan transparansi dan keandalan penyimpanan. Pendekatan ini dinilai efektif sebagai solusi penyimpanan data video berskala besar yang aman dan tahan terhadap gangguan.

Oleh karena itu, penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan CCTV berbasis blockchain dan IPFS guna memastikan bahwa data rekaman video tidak mudah dihilangkan, dimanipulasi, maupun dihapus secara sepihak, sehingga dapat meningkatkan keandalan dan keamanan sistem CCTV pada lingkungan rumah pintar.

2. TINJAUAN PUSTAKA

2.1. Internet of Things

Internet of things atau bisa disebut juga dengan IoT merupakan inovasi teknologi yang dirancang untuk mengoptimalkan konektivitas internet secara berkelanjutan guna mempermudah aktivitas manusia melalui integrasi benda-benda di sekitar[5]. Implementasi IoT yang kian meluas di berbagai sektor kehidupan menegaskan urgensi teknologi ini. Secara teknis, meski sering diidentikkan dengan metode komunikasi berbasis RFID (*Radio Frequency Identification*), cakupan IoT sebenarnya lebih luas, meliputi penggunaan sensor, teknologi nirkabel, hingga kode QR (Laghari et al., 2021)

Secara terminologi, *Internet of Things* (IoT) terbagi menjadi dua elemen fundamental: "*Internet*" sebagai infrastruktur pengatur konektivitas, dan "*Things*" yang merepresentasikan objek atau perangkat fisik[6]. Konsep dasarnya adalah memfungsikan perangkat-perangkat tersebut agar mampu berinteraksi, menghimpun informasi, serta mentransmisikannya melalui jaringan internet. Data ini juga dapat diakses oleh "*Things*" lainnya juga, dimana sebuah "*Things*" tertentu memiliki kemampuan untuk mengirimkan data lewat melalui jaringan dimanapun kamu berada dan tanpa adanya interaksi dari manusia ke manusia ataupun dari manusia ke perangkat komputer (Selay et al., 2022).

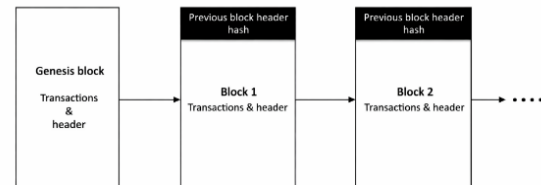
Internet of Things (IoT) merupakan bagian integral dari ekosistem internet global yang menghubungkan berbagai objek secara luas[5]. Dalam sistem ini, setiap entitas terintegrasi dengan perangkat yang dilengkapi teknologi sensor untuk memungkinkan komunikasi data. Adapun fungsi dasar dari Internet of Things adalah:

- Tagging (Penandaan)**
Proses klasifikasi atau pemberian identitas pada data yang telah dihimpun agar mudah dikelola.
- Monitoring (Pemantauan)**
Pengawasan secara berkala dan real-time terhadap jalannya suatu aktivitas atau sistem.
- Tracking (Pelacakan)**
Fungsi untuk memantau perpindahan atau posisi geografis dari suatu objek secara akurat.
- Control (Pengendalian)**
Upaya mempertahankan parameter atau kondisi sistem tertentu melalui pengaturan instruksi yang telah ditetapkan.
- Analysis (Analisis)**
Tahap pemrosesan data untuk menemukan solusi atas suatu persoalan serta menyajikan umpan balik yang relevan bagi pengguna

2.2. Blockchain

Secara sederhana *blockchain* adalah sebuah rantai blok yang berisi kumpulan data transaksi yang disusun secara kronologis dan terhubung satu sama lain menggunakan teknik kriptografi[7]. Setiap blok berisi sejumlah transaksi, cap waktu dan informasi tentang

blok sebelumnya dalam bentuk *hash*, yang menjamin integritas dan keamanan data. Dengan struktur ini, data dalam *blockchain* sangat sulit untuk diubah atau dimanipulasi tanpa persetujuan jaringan secara keseluruhan, sehingga *blockchain* sering dianggap sebagai teknologi yang transparan dan tahan terhadap penipuan[8].



Gambar 1. Struktur umum *blockchain*

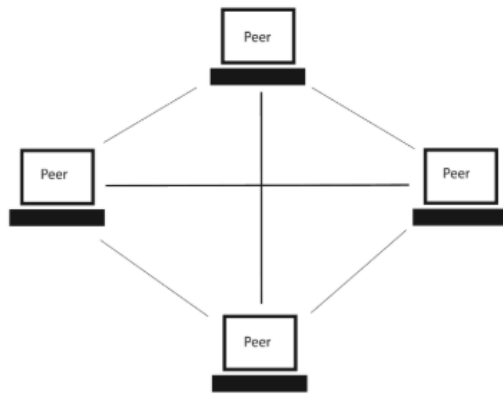
Hal-hal yang akan ditemui yang berhubungan dengan *blockchain* (Dr. Phil. Dony Novaliendry, n.d.):

- Alamat:** pengidentifikasi unik yang digunakan dalam transaksi *blockchain* untuk menunjukkan pengirim dan penerima. Alamat biasanya merupakan kunci public atau berasal dari kunci public.
- Transaksi:** unit fundamental dari sebuah *blockchain*. Transaksi mewakili transfer nilai dari satu alamat ke alamat lainnya.
- Blok:** sebuah blok terdiri dari beberapa transaksi dan elemen lainnya, seperti hash blok sebelumnya, stempel waktu, dan nonce. Sebuah blok berisi beberapa elemen, yaitu: referensi blok sebelumnya, nonce (nomor yang dihasilkan dan digunakan hanya sekali), waktu pembuatan blok (timestamp), hash dari semua node pohon Merkle (merkel root), dan badan blok.

2.3. IPFS (InterPlanetary File System)

InterPlanetary File System (IPFS) merupakan protokol jaringan peer-to-peer (P2P) yang memfasilitasi penyimpanan informasi secara terdesentralisasi[9]. Dengan mendistribusikan file ke berbagai node dalam jaringan, IPFS mampu mengeliminasi ketergantungan pada server pusat serta meminimalisir beban kerja server konvensional. Melalui sistem distribusi ini, data dapat diakses dengan lebih cepat dan aman tanpa terikat pada satu titik penyimpanan saja[10].

IPFS menggunakan content identifier untuk secara unik mengidentifikasi setiap file dalam namespace global yang menghubungkan host IPFS. Dalam ekosistem IPFS, setiap dokumen diidentifikasi melalui nilai hash unik yang memungkinkan data tersebut diakses dari simpul (node) mana pun di dalam jaringan[11]. Sistem ini menganut prinsip kesetaraan antar-node, di mana setiap titik memiliki peran dan kapasitas yang sama dalam proses penyimpanan serta pengambilan informasi[10].

Gambar 2. Jaringan *peer-to-peer* pada IPFS

Setiap perubahan pada konten file sama sekali akan memberikan CID yang beda saat di-upload. Hal ini memastikan bahwa file yg di-upload ke IPFS tidak dapat diubah karena setiap perubahan akan menghasilkan Content Identifier baru yang unik. Satu CID dapat mewakili satu file atau folder[10].

Gateway IPFS HTTP menggunakan protocol TTP untuk menyajikan konten yg dihosting di jaringan IPFS, menjembatani kesenjangan antara dua protocol yang berbeda. Ini berarti kita dapat mengakses konten di IPFS melalui IPFS CID-nya. Gateway IPFS bisa bersifat lokal, private, atau public, dan menggunakan CID IPFS untuk menyediakan link URL. Untuk akses ke konten yang disimpan secara sederhana[10].

Tabel 1. *Gateway* IPFS

No	Gateway
1.	<a href="https://gateway.pinata.cloud/ipfs/<CID>">https://gateway.pinata.cloud/ipfs/<CID>
2.	<a href="https://dget.top/ipfs/<CID>">https://dget.top/ipfs/<CID>
3.	<a href="https://dweb.link/ipfs/<CID>">https://dweb.link/ipfs/<CID>

Implementasi IPFS menawarkan sejumlah keunggulan signifikan, di antaranya adalah peningkatan aspek keamanan. Hal ini dikarenakan data tidak terpusat pada satu lokasi, sehingga risiko penghapusan sepihak oleh otoritas tertentu dapat diminimalisir[12]. Selain itu, IPFS mengoptimalkan kecepatan transfer data melalui pengambilan berkas dari node terdekat dengan pengguna. Protokol ini juga mendukung fitur versioning, yang memungkinkan pengguna untuk mengelola serta mengakses berbagai versi dokumen, baik versi terdahulu maupun yang terbaru[5].

2.4. Penelitian Terdahulu

Penelitian mengenai integrasi blockchain dan InterPlanetary File System (IPFS) dalam sistem IoT telah banyak dilakukan untuk mengatasi permasalahan keamanan, privasi, dan ketergantungan pada penyimpanan terpusat. Liu et al. dalam A Secure Framework for IoT-Based Healthcare mengusulkan kerangka keamanan IoT pada sektor kesehatan dengan memanfaatkan blockchain sebagai mekanisme pencatatan data dan kontrol akses, serta penyimpanan off-chain untuk mengurangi beban blockchain. Hasil

penelitian menunjukkan bahwa sistem yang diusulkan mampu meningkatkan integritas data, mencegah manipulasi, dan memperkuat privasi informasi sensitif perangkat IoT[13].

Penelitian lain oleh Singh et al. berjudul Decentralized Trusted Storage of Audio-Video Log Data Based on Blockchain Technology and IPFS secara khusus membahas penyimpanan data audio dan video IoT menggunakan IPFS sebagai media penyimpanan terdistribusi, sedangkan blockchain digunakan untuk menyimpan hash data sebagai bukti keaslian. Penelitian ini membuktikan bahwa kombinasi blockchain dan IPFS efektif dalam menjaga keutuhan rekaman multimedia, menghindari single point of failure, serta meningkatkan transparansi dan kepercayaan terhadap data log audio-video[4].

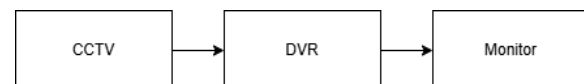
Sementara itu, Li et al. dalam penelitian Three-tier Storage Framework Based on TBchain and IPFS for Protecting IoT Security and Privacy mengusulkan arsitektur penyimpanan tiga lapis berbasis blockchain privat (TBchain) yang terhubung dengan IPFS. Model ini bertujuan meningkatkan skalabilitas dan efisiensi penyimpanan data IoT dengan memisahkan proses penyimpanan data besar dari blockchain utama. Hasil pengujian menunjukkan bahwa kerangka kerja tersebut mampu meningkatkan keamanan, menjaga privasi data pengguna, serta menyediakan mekanisme kontrol akses yang lebih baik terhadap data IoT[12].

Berdasarkan penelitian-penelitian tersebut, dapat disimpulkan bahwa penggunaan blockchain dan IPFS merupakan solusi yang menjanjikan untuk sistem keamanan dan penyimpanan data IoT. Namun, sebagian penelitian masih difokuskan pada simulasi atau sektor tertentu, sehingga penelitian ini berfokus pada implementasi nyata sistem penyimpanan rekaman CCTV rumah pintar berbasis blockchain dan IPFS sebagai pengembangan lebih lanjut.

3. METODE PENELITIAN

3.1. Analisa Sistem Berjalan

Analisis sistem berjalan dalam penelitian ini bertujuan untuk mengetahui alur kerja, proses perekaman, penyimpanan, serta pemantauan data video yang digunakan. Berikut gambaran umum alur sistem CCTV yang berjalan saat ini ditunjukkan pada Gambar 2.



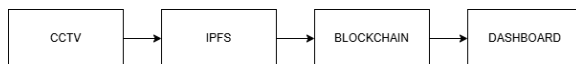
Gambar 3. Analisa Sistem Berjalan

Pada gambar 3 dijelaskan. Sistem CCTV yang berjalan saat ini, proses perekaman dan penyimpanan data masih dilakukan secara terpusat. CCTV berfungsi sebagai perangkat perekam yang menangkap aktivitas di area pemantauan dan mengirimkan data rekaman video ke perangkat Digital Video Recorder (DVR). DVR berperan sebagai media penyimpanan utama yang menampung seluruh rekaman video dalam jangka waktu tertentu. Data yang tersimpan pada DVR

selanjutnya dapat diakses oleh pengguna melalui monitor untuk keperluan pemantauan secara langsung maupun pemutaran ulang rekaman[5].

3.2. Analisa Sistem Usulan

Sistem usulan pada penelitian ini dirancang untuk mengatasi kelemahan sistem CCTV konvensional dengan menerapkan teknologi penyimpanan terdesentralisasi dan blockchain. Pasa sistem usulan ini terdiri dari beberapa komponen utama yang saling terintegrasi, yaitu CCTV, IPFS, Blockchain, dan perangkat monitoring. Setiap komponen memiliki peran dan fungsi masing-masing dalam mendukung kinerja sistem secara keseluruhan.



Gambar 4. Analisa Sistem Usulan

Keterangan gambar 4:

- CCTV**
CCTV berfungsi sebagai perangkat IoT yang melakukan perekaman aktivitas pada area pemantauan. Data yang dihasilkan berupa rekaman video digital yang selanjutnya dikirimkan ke sistem penyimpanan. Pada sistem ini, CCTV tidak menyimpan data secara permanen, sehingga dapat mengurangi risiko kehilangan data akibat kerusakan atau kegagalan perangkat. CCTV yang digunakan dalam penelitian ini merupakan CCTV berbasis IP Camera yang terhubung ke jaringan Wi-Fi, sehingga memungkinkan proses pengiriman data dilakukan melalui jaringan internet.
- IPFS**
IPFS berperan sebagai media penyimpanan data rekaman video secara terdesentralisasi. Data yang diterima dari CCTV disimpan dalam jaringan IPFS dan menghasilkan Content Identifier (CID) berupa hash unik. Penyimpanan terdesentralisasi ini menghilangkan ketergantungan pada satu server pusat dan meningkatkan ketahanan sistem terhadap kehilangan data.
- Blockchain**
Blockchain digunakan untuk menyimpan hash (CID) yang dihasilkan oleh IPFS melalui mekanisme smart contract. Pencatatan hash pada blockchain bersifat permanen dan tidak dapat diubah, sehingga berfungsi sebagai bukti keaslian dan integritas data rekaman video. Dengan demikian, setiap perubahan atau manipulasi data dapat terdeteksi dengan mudah.
- Arsip**
Arsip berfungsi sebagai antarmuka bagi pengguna untuk mengakses rekaman video

3.3. Perancangan Penelitian

Pada tahap ini akan dijelaskan tahapan kerja sistem secara terstruktur mulai dari proses perekaman hingga proses verifikasi data rekaman CCTV. Proses

ini dirancang untuk memastikan bahwa data rekaman video dapat disimpan secara aman, terdesentralisasi, serta memiliki jaminan integritas melalui pencatatan hash pada blockchain.



Gambar 4. Analisa Sistem Berjalan

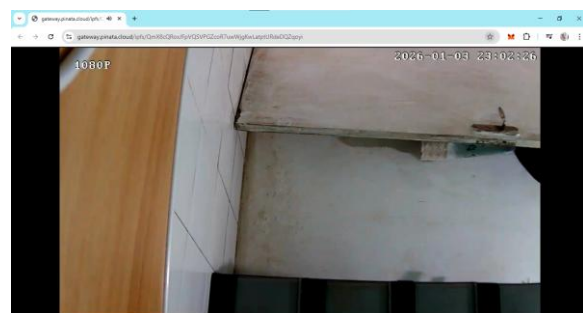
Keterangan alur:

- CCTV akan merekam dan menghasilkan video dengan format mp4, lalu disimpan sementara dalam penyimpanan lokal laptop.
- Penyimpanan lokal menerima hasil rekaman dari CCTV dan diteruskan ke IPFS untuk mendapatkan CID.
- IPFS akan memproses rekaman video sehingga mendapatkan CID, lalu akan dipin dalam pinata supaya hasil rekaman dapat ditampilkan pada dashboard. Setelah mendapatkan CID, akan dilanjutkan untuk pencatatan CID di blockchain.
- Blockchain menerima CID dari IPFS, lalu mencatatnya dalam node, serta dilanjutkan ke dashboard.
- Dashboard akan menampilkan waktu kapan rekaman disimpan dalam blockchain dan CID akan tertera sebagai bukti bahwa rekaman telah terdistribusi tidak lagi disimpan dalam lokal

4. HASIL DAN PEMBAHASAN

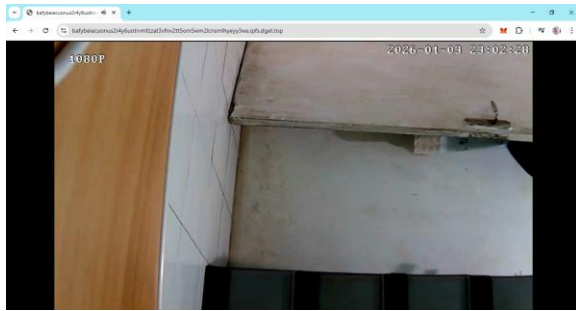
4.1. Pengujian Distribusi Data

Pengujian ini dilakukan untuk membuktikan bahwa sistem penyimpanan rekaman CCTV tidak lagi bergantung pada penyimpanan microSD atau NVR dan DVR, melainkan memanfaatkan mekanisme distribusi data pada jaringan InterPlanetary File System (IPFS). CID akan di akses dengan 3 gateway IPFS.



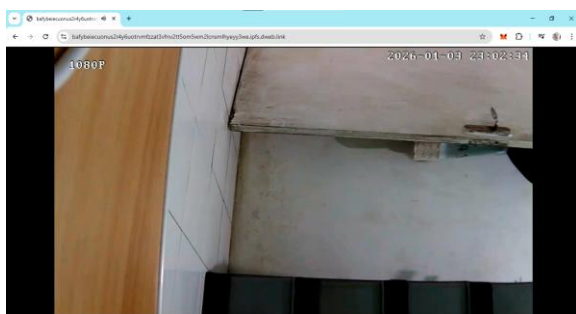
Gambar 5. Akses dengan gateway.pinata.cloud

Pada Gambar 5, hasil dari pengujian distribusi data. CID dapat di akses melalui gateway.pinata.cloud.



Gambar 6. Akses dengan dget.top

Pada Gambar 6, hasil dari pengujian distribusi data. CID dapat di akses melalui gateway dget.top.



Gambar 7. akses dengan dweb.link

Pada Gambar 7, hasil dari pengujian distribusi data. CID dapat di akses melalui gateway dweb.link.

Tabel 2. Uji coba gateway IPFS

No	Gateway	Status
1.	gateway.pinata.cloud	Berhasil diakses
2.	dget.top	Berhasil diakses
3.	dweb.link	Berhasil diakses

Berdasarkan Gambar 5, Gambar 6, Gambar 7, serta Tabel 2, dapat dibuktikan bahwa sistem penyimpanan rekaman CCTV yang diusulkan telah menerapkan mekanisme penyimpanan terdistribusi. Data rekaman tidak lagi disimpan secara lokal atau terpusat pada satu media penyimpanan tertentu, melainkan direpresentasikan dalam bentuk Content Identifier (CID) dan didistribusikan melalui jaringan IPFS. Hasil pengujian menunjukkan bahwa data rekaman dapat diakses melalui berbagai gateway IPFS dengan CID yang sama, sehingga membuktikan bahwa sistem tidak bergantung pada penyimpanan lokal dan memiliki tingkat ketersediaan data yang lebih tinggi dibandingkan sistem penyimpanan konvensional

4.2. Evaluasi dan Pembahasan

Berdasarkan hasil implementasi dan pengujian sistem yang telah dilakukan, dapat dievaluasi bahwa sistem keamanan IoT rumah pintar berbasis IPFS dan blockchain ini telah berhasil menerapkan konsep desentralisasi dalam penyimpanan dan pencatatan data

rekaman CCTV. Proses perekaman video berjalan secara periodik dengan durasi yang telah ditentukan, kemudian data tersebut diproses secara otomatis oleh backend tanpa intervensi manual. Hal ini menunjukkan bahwa sistem mampu bekerja secara berkelanjutan dan mandiri sesuai dengan kebutuhan lingkungan rumah pintar.

Pada tahap penyimpanan data, pemanfaatan InterPlanetary File System (IPFS) melalui layanan pinning Pinata terbukti mampu mengatasi permasalahan ketergantungan terhadap penyimpanan lokal. Setiap rekaman video yang diunggah ke IPFS menghasilkan Content Identifier (CID) yang bersifat unik dan merepresentasikan isi data secara keseluruhan. Hasil pengujian menunjukkan bahwa rekaman video dapat diakses kembali menggunakan CID yang sama, selama file tersebut tidak mengalami perubahan. Dengan demikian, IPFS berperan efektif sebagai media penyimpanan terdistribusi yang mendukung ketersediaan dan ketahanan data.

Selanjutnya, pencatatan CID ke dalam blockchain melalui smart contract menunjukkan bahwa sistem mampu menjamin integritas dan keaslian data rekaman CCTV. Setiap CID yang berhasil dicatat ke blockchain akan tersimpan secara permanen bersama dengan informasi waktu pencatatan. Karena sifat blockchain yang tidak dapat dimodifikasi, data CID yang telah dicatat tidak dapat diubah atau dihapus, sehingga memberikan jaminan keamanan terhadap kemungkinan manipulasi data. Apabila terjadi perubahan pada file rekaman, perbedaan hash dapat segera terdeteksi saat dilakukan verifikasi, yang menandakan bahwa data tidak lagi sesuai dengan data asli yang tercatat.

Dari sisi distribusi data, hasil pengujian yang ditunjukkan pada Gambar 5, Gambar 6, dan Gambar 7 serta Tabel 2 membuktikan bahwa sistem ini tidak lagi bergantung pada penyimpanan lokal atau server tunggal. Data rekaman disimpan secara terdistribusi pada jaringan IPFS, sementara metadata berupa CID dicatat di blockchain. Kombinasi kedua teknologi ini menghasilkan sistem yang lebih andal, transparan, dan tahan terhadap kegagalan sistem terpusat, sehingga mendukung tujuan utama penelitian.

Selain itu, antarmuka pengguna (dashboard) yang dikembangkan mampu menampilkan riwayat penyimpanan data rekaman CCTV secara jelas dan informatif. Pengguna dapat melihat waktu perekaman serta mengakses rekaman video melalui gateway IPFS berdasarkan CID yang tersimpan di blockchain. Hal ini menunjukkan bahwa sistem tidak hanya berfungsi dari sisi teknis, tetapi juga mudah digunakan oleh pengguna akhir dalam memantau keamanan rumah pintar.

Secara keseluruhan, hasil evaluasi menunjukkan bahwa integrasi IPFS dan blockchain pada sistem keamanan IoT rumah pintar ini telah berjalan sesuai dengan perancangan. Meskipun masih terdapat keterbatasan, seperti penggunaan jaringan blockchain privat dan belum diterapkannya streaming video

secara real-time, sistem yang dibangun telah berhasil membuktikan konsep desentralisasi penyimpanan dan pencatatan data CCTV secara aman, transparan, dan dapat dipertanggungjawabkan

5. KESIMPULAN DAN SARAN

Sistem penyimpanan rekaman CCTV berbasis integrasi blockchain dan InterPlanetary File System (IPFS) berhasil diimplementasikan sebagai solusi penyimpanan terdistribusi yang tidak bergantung pada media lokal maupun server terpusat. Rekaman video CCTV disimpan melalui IPFS, sementara blockchain digunakan untuk mencatat Content Identifier (CID) yang bersifat unik dan merepresentasikan konten video secara kriptografis, sehingga setiap perubahan data dapat terdeteksi dan integritas serta keaslian data tetap terjaga. Hasil pengujian menunjukkan bahwa data rekaman dapat didistribusikan dan diakses melalui berbagai gateway IPFS tanpa bergantung pada satu lokasi penyimpanan tertentu, yang membuktikan sifat desentralisasi sistem. Selain itu, antarmuka pengguna yang dibangun mampu menampilkan riwayat penyimpanan, waktu perekaman, serta tautan akses video melalui IPFS, sehingga memudahkan pengguna dalam memantau dan mengelola data rekaman CCTV secara efektif.

DAFTAR PUSTAKA

- [1] S. S. M. S. Ade Putra Ode Amame *et al.*, *PEMANFAATAN DAN PENERAPAN INTERNET OF THINGS (IOT) DI BERBAGAI BIDANG*. PT. Sonpedia Publishing Indonesia, 2023. [Online]. Available: <https://books.google.co.id/books?id=8zWqEAAQBAJ>
- [2] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "BlockMedCare : A healthcare system based on IoT , Blockchain and IPFS for data management security," *Egypt. Informatics J.*, vol. 23, no. 2, pp. 329–343, 2022, doi: 10.1016/j.eij.2022.02.004.
- [3] B. Irawan and D. Trihatmojo, "Decentralized Trusted Storage of Audio-Video Log Data Based on Blockchain Technology and IPFS," *Int. J. Sci. Technol. Manag.*, vol. 5, no. 2, pp. 473–484, 2024, doi: <https://doi.org/10.46729/ijstm.v5i2.1084>.
- [4] S. N. Mahmud, "Revolusi Internet of Things (IoT) dalam Arsitektur : Menghubungkan Bangunan dengan Dunia Digital," pp. 1–12.
- [5] F. Ramadandi, "Pengembangan Sistem Smart Home Berbasis Internet Of Things Untuk Mengontrol Peralatan Elektronik," vol. 2, pp. 171–178, 2024.
- [6] S. K. M. K. Dr. Phil. Dony Novaliendry, *MENGUASAI BLOCKCHAIN Cara Kerja Blockchain, Mulai Dari Kriptografi dan Identitas Terdesentralisasi, Hingga DeFi, NFT, dan Web3 JILID 1*. Penerbit CV. SARNU UNTUNG. [Online]. Available: <https://books.google.co.id/books?id=3DVJEQAQBAJ>
- [7] M. Faqih Febriansyah, R. Setiawan, and T. Sutabri, "Kemudahan dan Keamanan Dalam Rumah Pintar: Tinjauan Terhadap Teknologi Smart Home," *IJM Indones. J. Multidiscip.*, vol. 2, pp. 24–31, 2024, [Online]. Available: <https://journal.csspublishing/index.php/ijm>
- [8] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H. N. Lee, "Ethereum Smart Contract Analysis Tools: A Systematic Review," *IEEE Access*, vol. 10, pp. 57037–57062, 2022, doi: 10.1109/ACCESS.2022.3169902.
- [9] A. A. Laghari, K. Wu, R. Ali, L. Mureed, A. Abdullah, and A. Khan, "A Review and State of Art of Internet of Things (IoT) A Review and State of Art of Internet of Things (IoT)," *Arch. Comput. Methods Eng.*, no. July, 2021, doi: 10.1007/s11831-021-09622-6.
- [10] N. Manoj and P. Kumar, "Blockchain technology for security issues and challenges in IoT," *Procedia Comput. Sci.*, vol. 132, pp. 1815–1823, 2018, doi: 10.1016/j.procs.2018.05.140.
- [11] Y. Li, Y. Yu, and X. Wang, "Three-tier Storage Framework Based on TBchain and IPFS for Protecting IoT Security and Privacy Three-tier Storage Framework Based on TBchain and IPFS for Protecting IoT Security and Privacy," *ACM Trans. Internet Technol.*, vol. 23, no. 3, pp. 36–65, 2023, doi: 10.1145/3549910.
- [12] D. Rani, "A secure framework for IoT-based healthcare using blockchain and IPFS," *Wiley*, vol. 7, no. 2, pp. 1–25, 2023, doi: <https://doi.org/10.1002/spy2.348>.