IMPLEMENTASI BLOCKCHAIN DALAM SISTEM KEAMANAN JARINGAN UNTUK MENDETEKSI SERANGAN SIBER DISTRIBUTED DENIAL OF SERVICE (DDOS)

Eryagiandi Septiawan, Bambang Irawan
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Esa Unggul
Jl. Arjuna Utara No.9, Kebon Jeruk, Jakarta, Indonesia
eryagiandi@student.esaunggul.ac.id

ABSTRAK

Perkembangan teknologi informasi yang pesat meningkatkan ketergantungan terhadap jaringan komputer, sehingga keamanan jaringan menjadi aspek yang sangat penting untuk diperhatikan. Salah satu ancaman yang sering terjadi adalah serangan *Distributed Denial of Service* (DDoS) yang dapat mengganggu ketersediaan layanan jaringan dengan membanjiri *server* menggunakan lalu lintas data dalam jumlah besar. Penelitian ini bertujuan untuk mengimplementasikan teknologi *blockchain* dalam sistem keamanan jaringan guna mendeteksi aktivitas yang berpotensi sebagai serangan DDoS serta meningkatkan transparansi dan integritas data. Metode yang digunakan dalam penelitian ini adalah *Rapid Application Development* (RAD) untuk mempercepat proses pengembangan sistem. Sistem dibangun menggunakan *React.js* pada sisi *frontend*, *Flask* pada *backend*, serta *smart contract* berbasis *Ethereum* yang dijalankan pada jaringan *Sepolia Testnet*. Hasil penelitian menunjukkan bahwa sistem mampu memantau aktivitas jaringan, mencatat alamat *IP* yang terdeteksi secara aman ke dalam *blockchain*, serta menyimpan *log* aktivitas pada *MongoDB*. Proses transaksi pada *blockchain* memerlukan waktu konfirmasi rata-rata sekitar 12 detik dengan biaya transaksi berkisar antara 0,0005 hingga 0,0006 *SepoliaETH*. Implementasi ini menunjukkan bahwa *blockchain* dapat meningkatkan transparansi, keamanan data, dan ketahanan sistem terhadap potensi serangan siber.

Kata kunci : *Blockchain; Network Security; Distributed Denial of Service; Smart Contract; Decentralized*

1. PENDAHULUAN

Pada era digital, berbagai sektor telah memanfaatkan teknologi informasi secara luas. Akibatnya, semakin banyak individu yang bergantung pada teknologi komputer yang memerlukan konektivitas internet secara berkelanjutan [1]. Oleh karena itu, perlindungan terhadap privasi dan integritas data di berbagai bidang menjadi suatu keharusan [2]. Sistem keamanan informasi berfungsi untuk melindungi seluruh aset informasi dari akses atau penggunaan yang tidak sah [3]. Sistem ini bertujuan untuk memastikan bahwa akses terhadap data hanya diberikan kepada pihak-pihak yang berwenang [4].

Masih terdapat berbagai isu, ancaman, dan permasalahan keamanan, salah satunya adalah serangan *Distributed Denial of Service* (DDoS) [5]. Serangan DDoS bukanlah fenomena baru, namun hingga saat ini tetap menjadi permasalahan besar dalam ranah keamanan siber [6]. Serangan siber jenis ini termasuk yang paling berbahaya karena frekuensi kejadiannya yang tinggi serta banyaknya laporan insiden yang terjadi [7]. Serangan DDoS merupakan bentuk ancaman siber yang membanjiri *server* atau jaringan dengan lalu lintas yang berlebihan sehingga menyebabkan sistem tidak dapat beroperasi secara normal [8]. Jenis serangan ini dilakukan dengan mengirimkan data atau permintaan dalam jumlah yang sangat besar ke target, sehingga sistem kesulitan untuk memprosesnya dengan baik [9]. Akibatnya, *server* dapat mengalami peningkatan waktu respons secara signifikan atau bahkan berhenti beroperasi sama sekali [10].

Serangan DDoS dapat menimbulkan dampak yang sangat merugikan bagi perusahaan, baik dari segi finansial, kerusakan reputasi, maupun gangguan operasional yang signifikan [11]. Untuk melindungi jaringan dari ancaman siber, terdapat beberapa mekanisme keamanan yang umum digunakan, di antaranya *firewall* dan *Intrusion Detection System* (IDS) [12]. *Firewall* berfungsi sebagai penghalang untuk mencegah akses yang tidak sah, sedangkan IDS bertugas mendeteksi aktivitas yang mencurigakan atau tidak normal dalam jaringan [13].

Sistem *blockchain* tidak dimiliki oleh individu maupun kelompok tertentu. Teknologi ini memungkinkan proses pengiriman dan penyimpanan data secara aman tanpa mengubah keasliannya. *Blockchain* merupakan kumpulan blok yang saling terhubung satu sama lain [14]. Kriptografi digunakan untuk menjaga keamanan setiap blok, sementara node dalam jaringan mencapai kesepakatan (*consensus*) guna memastikan sistem tetap aman dan andal [15]. Data yang telah tersimpan di dalam blok tidak dapat diubah [16]. Oleh karena itu, proses pembaruan data menjadi sulit dilakukan tanpa tetap menjaga keabsahan dan integritasnya sesuai dengan mekanisme yang telah ditetapkan [17].

Blockchain merupakan teknologi baru yang telah dimanfaatkan dalam berbagai bidang [18]. Teknologi ini awalnya dikembangkan untuk mempermudah transaksi mata uang *crypto* seperti *Bitcoin*, namun saat ini juga digunakan untuk berbagai keperluan lain, seperti *smart contract* dan sistem identifikasi digital [19]. Dalam perkembangannya, sistem keamanan informasi mulai mengadopsi teknologi *blockchain*

untuk meningkatkan keandalan data, menjaga kerahasiaan, serta memperkuat integritas informasi [20].

Berdasarkan permasalahan tersebut, diperlukan suatu pendekatan yang mampu meningkatkan efektivitas sistem keamanan jaringan dalam mendeteksi serangan DDoS. Teknologi *blockchain* menawarkan karakteristik desentralisasi, transparansi, serta sifat data yang tidak dapat diubah (*immutable*) sehingga berpotensi meningkatkan keandalan sistem keamanan jaringan. Dengan memanfaatkan mekanisme kriptografi dan pencatatan transaksi yang permanen, *blockchain* dapat digunakan untuk memantau aktivitas jaringan dan mendokumentasikan kejadian serangan secara aman. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan teknologi *blockchain* dalam sistem keamanan jaringan guna mendeteksi dan mencatat aktivitas yang berpotensi sebagai serangan DDoS. Sistem yang dikembangkan diharapkan mampu meningkatkan transparansi data, memperkuat integritas informasi, serta memberikan mekanisme deteksi yang lebih efektif terhadap ancaman siber.

Terdapat berbagai manfaat utama dari penerapan teknologi *blockchain* dalam sistem keamanan informasi [21]. Manfaat tersebut meliputi peningkatan perlindungan data, pemeliharaan keakuratan informasi, dukungan terhadap anonimitas pengguna, peningkatan transparansi proses dan transaksi, serta jaminan penyimpanan data yang lebih aman [22]. Penelitian ini mengkaji penerapan teknologi *blockchain* pada sistem keamanan jaringan untuk mendeteksi serangan DDoS. Solusi yang diusulkan memanfaatkan teknologi *blockchain* guna meningkatkan efektivitas dan mempercepat upaya perlindungan jaringan komputer terhadap ancaman siber yang terus berkembang.

2. TINJAUAN PUSTAKA

Berbagai penelitian telah mengeksplorasi pemanfaatan teknologi *blockchain* untuk mengidentifikasi ancaman *Distributed Denial of Service* (DDoS) melalui beragam pendekatan. Salah satu penelitian mengembangkan *BSD-Guard*, yaitu solusi berbasis *blockchain* yang bersifat kolaboratif untuk mendeteksi dan mencegah serangan DDoS pada lingkungan *Software-Defined Networking* (SDN). Pendekatan ini mempermudah kolaborasi antar pemangku kepentingan serta memastikan bahwa data deteksi bersifat transparan dan akurat [23].

Penelitian lain mengusulkan mekanisme kolaboratif dengan memanfaatkan *Interplanetary File System* (IPFS) sebagai media penyimpanan data yang lebih efisien. Pendekatan tersebut mampu meningkatkan kecepatan serta menekan biaya dalam proses transmisi dan penyimpanan data, sehingga mendukung deteksi serangan DDoS melalui pengelolaan data yang terdesentralisasi [24].

Selain itu, sejumlah kajian juga meneliti penggunaan teknologi *blockchain* untuk melindungi ekosistem *Internet of Things* (IoT) dari serangan DDoS. Penelitian tersebut mengelompokkan solusi ke dalam empat kategori utama, yaitu arsitektur terdistribusi, manajemen akses, pengendalian lalu lintas, dan platform berbasis *Ethereum*. Hasil penelitian menunjukkan bahwa pendekatan manajemen akses dan pengendalian lalu lintas merupakan metode yang paling efektif untuk diterapkan pada aplikasi *IoT* [25].

Dalam penelitian lainnya, peneliti menggunakan *testbed* berbasis *blockchain-IoT* untuk mengevaluasi dampak serangan DDoS terhadap perangkat *IoT*. Hasil penelitian menunjukkan bahwa serangan DDoS dapat meningkatkan suhu perangkat hingga lebih dari 90°C serta menyebabkan tingkat kehilangan blok (*block loss rate*) mencapai 81,3%, yang secara signifikan memperlambat kinerja jaringan [26].

Penelitian lain memanfaatkan model teori permainan (*game-theoretic models*) untuk menganalisis kemungkinan respons para *miner* terhadap serangan DDoS yang menargetkan *mining pool*. Hasil kajian menunjukkan bahwa strategi para miner dapat berubah dari *defensif* menjadi *ofensif*, bergantung pada kondisi jaringan yang sedang berlangsung. Selain itu, penelitian tersebut juga menunjukkan bahwa model permainan evolusioner dinamis menghasilkan analisis yang lebih akurat dibandingkan dengan model statis [27][28].

Penelitian tersebut memanfaatkan kombinasi *Artificial Neural Networks* (ANN), teknologi *blockchain*, dan *multi-controller Software-Defined Networking* (SDN) untuk mendeteksi serta menghentikan serangan DDoS pada jaringan *IoT*. Melalui penerapan keamanan terdesentralisasi dan analisis pola serangan yang lebih baik, integrasi ini mampu meningkatkan manajemen jaringan serta mempermudah proses identifikasi ancaman [29].

Hasil kajian menunjukkan bahwa penggabungan teknologi *blockchain* dengan mekanisme deteksi DDoS dapat meningkatkan tingkat keamanan, transparansi, dan desentralisasi sistem. Meskipun demikian, sebagian besar penelitian sebelumnya masih bergantung pada kerangka konseptual atau data eksperimen yang terbatas. Penelitian ini berupaya mengembangkan kajian yang ada dengan mengimplementasikan *smart contract Ethereum* pada *Sepolia Testnet* untuk menyediakan mekanisme deteksi berbasis *blockchain*. Sistem ini memiliki kemampuan pencatatan kejadian serangan yang tidak dapat diubah (*immutable*), serta dapat diuji melalui simulasi serangan DDoS secara nyata guna mengevaluasi kinerja dan tingkat akurasinya.

3. METODE PENELITIAN

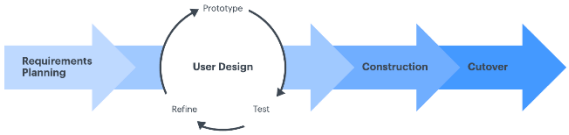
3.1. Metode Pengembangan Sistem

Rapid Application Development (RAD) merupakan metodologi pengembangan perangkat lunak yang menekankan pada proses pengembangan secara bertahap (*incremental*) dan iteratif. Pendekatan ini dinilai efektif untuk mempercepat penyelesaian

sistem [30]. Tahap awal dilakukan dengan mengidentifikasi permasalahan pada mekanisme keamanan jaringan konvensional. Selanjutnya, kebutuhan sistem ditentukan berdasarkan kajian literatur dari berbagai buku dan artikel ilmiah yang membahas serangan DDoS serta teknologi *blockchain*.

Tahap berikutnya adalah perancangan *prototipe* yang mencakup antarmuka pengguna, arsitektur data, serta modul yang terintegrasi dengan sistem *blockchain* untuk mendeteksi lalu lintas jaringan yang tidak normal. Sistem ini dirancang untuk memberikan pemahaman kepada pengguna mengenai mekanisme pencegahan serangan DDoS. Sebuah dashboard disediakan untuk memantau aktivitas sistem selama proses berlangsung, sementara *ledger blockchain* digunakan untuk mencatat setiap kejadian serangan secara permanen.

Tahap akhir dilakukan melalui pengujian simulasi untuk mengevaluasi kemampuan sistem dalam mendeteksi serangan DDoS sekaligus melindungi data. Tahapan ini menjadi dasar dalam proses evaluasi dan penyempurnaan sistem, sebagaimana diilustrasikan pada Gambar 1.



Gambar 1. *Rapid application development*

3.2. Instrumen Penelitian

Instrumen penelitian merupakan komponen penting dalam proses perancangan, pengujian, dan evaluasi solusi keamanan jaringan berbasis *blockchain* yang diusulkan. Penelitian ini menggunakan tiga lapisan utama instrumen, yaitu lapisan *blockchain*, *backend*, dan *frontend*. Setiap lapisan memanfaatkan perangkat atau teknologi yang berbeda, namun saling terintegrasi untuk membentuk suatu sistem yang utuh.

3.3. Blockchain

Lapisan *blockchain* merupakan komponen utama dalam proyek ini karena berfungsi untuk melindungi data serangan serta menjamin bahwa data tersebut tidak dapat diubah (*immutable*) [31]. Jaringan *Ethereum Sepolia* digunakan sebagai lingkungan uji yang menyerupai *public mainnet*, namun tetap aman dan bebas biaya untuk keperluan eksperimen. Pada jaringan ini, *smart contract* yang ditulis menggunakan bahasa *Solidity* berperan sebagai digital *ledger* yang mencatat setiap alamat IP yang terlibat dalam serangan DDoS sebagai sebuah transaksi, sehingga rekaman data tidak dapat dimodifikasi.

MetaMask digunakan sebagai dompet digital yang menghubungkan antarmuka pengguna secara langsung dengan *blockchain*, sekaligus melakukan proses verifikasi dan persetujuan transaksi. Sementara itu, *Truffle* berfungsi untuk menulis, menguji, dan menjalankan smart contract. Fitur ini membantu menjaga konsistensi proses pengembangan serta memudahkan replikasi penelitian.

3.4. Frontend

Lapisan frontend menyediakan antarmuka interaktif yang memungkinkan administrator jaringan untuk memantau sistem secara *real-time* [32]. Kerangka kerja *React.js* dipilih karena kemampuannya dalam menghadirkan pengalaman *single-page application* yang responsif. Komponen *React* secara dinamis menampilkan grafik lonjakan lalu lintas, tabel riwayat serangan, serta status koneksi ke *blockchain*.

Penggunaan *Ethers.js* berperan penting dalam menghubungkan aplikasi dengan *MetaMask*, menjalankan fungsi *smart contract* untuk mengambil data yang tersimpan, serta melakukan transaksi baru ketika diperlukan keterlibatan administrator. Integrasi antara *React.*js dan *Ethers.js* menghasilkan antarmuka yang informatif sekaligus memungkinkan interaksi langsung dengan jaringan blockchain tanpa memerlukan penggunaan terminal atau alat eksternal lainnya.

3.5. Backend

Pada lapisan *backend*, kerangka kerja *Flask* atau *Django*, bergantung pada kebutuhan skalabilitas aplikasidigunakan untuk menjalankan logika utama sistem [33]. Perangkat *Web3.py* memfasilitasi koneksi aplikasi dengan jaringan *Ethereum* dengan cara secara otomatis menghasilkan, menandatangani, dan mengirimkan transaksi [34]. Ketika pola serangan terdeteksi, Intrusion *Detection System* (IDS) terlebih dahulu mencatat detail kejadian, seperti *timestamp*, alamat IP, dan intensitas lalu lintas, ke dalam *MongoDB* sebagai penyimpanan sementara. Hal ini memungkinkan proses analisis atau penyajian informasi dilakukan dengan cepat tanpa harus menunggu konfirmasi dari blockchain.

Setelah proses verifikasi selesai, data yang sama diformat sebagai transaksi dan dikirimkan ke *smart contract*. Pendekatan ini menjamin adanya redundansi data sekaligus meningkatkan transparansi. Dalam arsitektur ini, backend berperan sebagai "orkestrator" yang memastikan proses deteksi secara real-time dan pencatatan permanen pada blockchain dapat berjalan secara bersamaan [35].

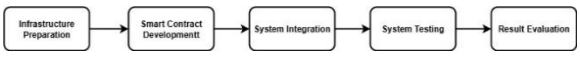
3.6. Proses Implementasi Sistem

Proses implementasi sistem merupakan tahapan dalam pengembangan sistem keamanan jaringan berbasis *blockchain* yang mampu menangani serangan DDoS. Tahap pertama adalah menyiapkan infrastruktur, yaitu dengan menggunakan *Ethereum Sepolia Testnet* sebagai jaringan *blockchain* utama dalam lingkungan operasional. Jaringan ini berfungsi menyerupai jaringan publik namun dapat digunakan tanpa biaya, sehingga sesuai untuk kebutuhan pengujian dan pengembangan. Selain itu, dilakukan simulasi jaringan lokal untuk memperoleh pengukuran aliran data secara akurat. Pada tahap ini juga dilakukan

instalasi seluruh dependensi yang diperlukan, seperti *Web3.py*, *Truffle*, *MetaMask*, serta *React.js* dan *Flask*.

Tahap selanjutnya adalah pengembangan smart contract menggunakan bahasa *Solidity* yang berfungsi mencatat data serangan, meliputi alamat IP, timestamp, dan status deteksi. Pengujian awal *smart contract* Truffle, kemudian dideploy ke *Sepolia Testnet* untuk mengevaluasi kinerjanya pada lingkungan yang menyerupai kondisi nyata. Setelah itu, seluruh komponen sistem diintegrasikan, di mana *backend* (*Python* dan *Web3.py*) mengambil data dari *blockchain* dan meneruskannya ke *frontend*. Antarmuka pengguna dibangun menggunakan *React.js* dan *Ethers.js* yang terhubung dengan *MetaMask* untuk memantau sistem secara langsung.

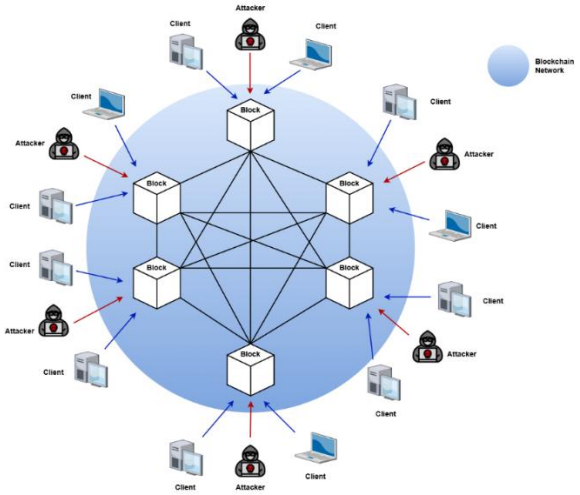
Tahap integrasi ini memastikan bahwa seluruh data serangan dapat dicatat dan diverifikasi secara aman. Setelah sistem terintegrasi, dilakukan pengujian dengan mensimulasikan serangan DDoS melalui pengiriman sejumlah besar permintaan ke *server*. Pengujian ini bertujuan untuk menilai kemampuan sistem dalam mendeteksi dan merekam aktivitas anomali ke dalam *smart contract*. Hasil pengujian dianalisis dengan membandingkan data yang tersimpan pada *blockchain* dengan *log* yang terdapat di *MongoDB*. Aspek lain yang dievaluasi meliputi kecepatan deteksi, akurasi pencatatan, stabilitas sistem, serta efektivitas antarmuka pengguna dalam melakukan pemantauan. Evaluasi ini memberikan dasar untuk menilai skalabilitas sistem. Implementasi sistem tersebut ditunjukkan pada Gambar 2.



Gambar 2. Proses implementasi sistem

3.7. Arsitektur Sistem Jaringan *Blockchain*

Setiap komponen dalam jaringan *blockchain* yang terdesentralisasi dan aman beroperasi secara mandiri di dalam ekosistem jaringan [36]. Arsitektur *peer-to-peer* (P2P) dibangun sebagai inti jaringan melalui sejumlah blok yang saling terhubung, di mana setiap blok berfungsi sebagai *node* yang menyimpan salinan lengkap seluruh data transaksi [37]. Node-node tersebut bertugas memantau, mencatat, dan mendistribusikan data secara cepat ke seluruh jaringan. Pendekatan ini memungkinkan tercapainya mekanisme konsensus tanpa memerlukan otoritas terpusat. Berbagai pengguna mengirimkan permintaan transaksi ke sistem *blockchain* dari sumber eksternal sebagai bukti bahwa data yang dikirimkan bersifat autentik. Namun demikian, terdapat pula pihak yang berpotensi menjadi ancaman dengan mencoba memanipulasi data dari luar sistem. Untuk memastikan keakuratan dan validitas setiap transaksi, *node* menggunakan mekanisme konsensus seperti *Proof of Work* (PoW) dan *Proof of Stake* (PoS) [38]. Melalui mekanisme tersebut, blockchain mampu mencegah serangan yang tidak sah sekaligus menjaga data tetap aman, terlindungi, transparan, dan andal dalam suatu ekosistem digital terbuka yang terpercaya [39]. Desain sistem jaringan *blockchain* ini ditunjukkan pada Gambar 3.



Gambar 3 Sistem jaringan blockchain untuk serangan DDoS

4. HASIL DAN PEMBAHASAN

Hasil implementasi sistem berhasil mengintegrasikan teknologi *blockchain* ke dalam kerangka kerja keamanan jaringan yang dirancang khusus untuk menghadapi ancaman *Distributed Denial of Service* (DDoS). Antarmuka aplikasi berbasis *React.js* digunakan untuk memindai lima alamat IP yang berbeda dalam suatu lingkungan simulasi.

Tingkat aktivitas yang terdeteksi bervariasi pada setiap proses pemindaian, dengan frekuensi ping berkisar antara 1 hingga 11, serta durasi pemindaian antara 10.275 milidetik hingga 69.663 milidetik. Meskipun tidak ditemukan lalu lintas berbahaya, setiap transaksi tetap terdokumentasi secara aman menggunakan *blockchain Ethereum* melalui *smart contract* serta *MetaMask* untuk proses autentikasi dan tanda tangan digital. Biaya transaksi tercatat berada pada rentang 0,00050055 hingga 0,00062905 *SepoliaETH*, dengan rata-rata waktu validasi sekitar 12 detik.

Bagian *backend* sistem, yang dikembangkan menggunakan *Python* dan *Flask*, terhubung dengan *MongoDB* untuk menyimpan *log* dari berbagai pengguna guna keperluan evaluasi administratif. Log tersebut memuat informasi timestamp, alamat IP, serta indikator status yang membantu dalam proses identifikasi pola dan mitigasi ancaman. Seluruh aktivitas pada *blockchain* dapat diakses secara publik melalui *Etherscan*, sehingga menjamin keterlacakan (*traceability*) dan sifat tidak dapat diubah (*immutability*) dari data.

Antarmuka *frontend* memungkinkan pemantauan secara *real-time*, pencatatan manual, serta ekspor laporan, sehingga memberikan informasi yang jelas dan bernilai bagi pengelola jaringan. Integrasi antara lapisan *frontend*, *backend*, dan *blockchain*

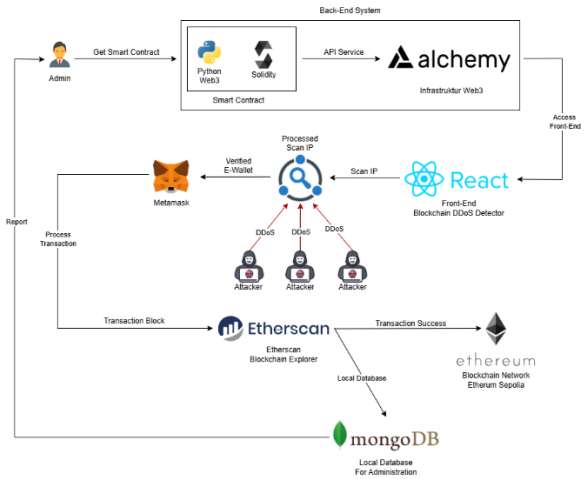
menunjukkan kekuatan arsitektur sistem yang dibangun. Hasil penelitian ini mengindikasikan bahwa sistem keamanan jaringan berbasis *blockchain* mampu secara efektif mengidentifikasi, mendokumentasikan, dan menampilkan insiden serangan, sehingga berpotensi untuk diterapkan secara lebih luas dalam bidang keamanan siber.

4.1. Arsitektur Sistem Aplikasi

Arsitektur sistem aplikasi ini menunjukkan bagaimana suatu sistem keamanan jaringan mendeteksi serangan DDoS dengan memanfaatkan teknologi *blockchain Ethereum*. Tahap awal dimulai dari melakukan perancangan dan pembuatan *smart contract* menggunakan bahasa *Solidity* serta kerangka kerja *Python Web3*. Kontrak tersebut dijalankan melalui layanan *API Alchemy* yang menghubungkan sistem dengan jaringan *Ethereum Sepolia Testnet*.

Setelah pengembangan *backend* selesai, administrator dapat mengoperasikan antarmuka pengguna yang dibangun menggunakan *React.js*. Antarmuka ini dilengkapi dengan fitur pemindai IP (*IP scanner*) dan pendeteksi DDoS yang dirancang untuk memantau lalu lintas jaringan serta mengidentifikasi alamat IP yang berpotensi menjadi sumber serangan. Ketika *MetaMask* mendeteksi aktivitas mencurigakan, sistem akan mengirimkan alamat IP penyerang ke *blockchain*. *MetaMask* kemudian memverifikasi dan menyetujui transaksi sebelum dicatat pada jaringan *Ethereum*. Setelah transaksi terkonfirmasi, informasi IP tersimpan secara permanen dan tidak dapat diubah, serta dapat diakses secara publik melalui *Etherscan*.

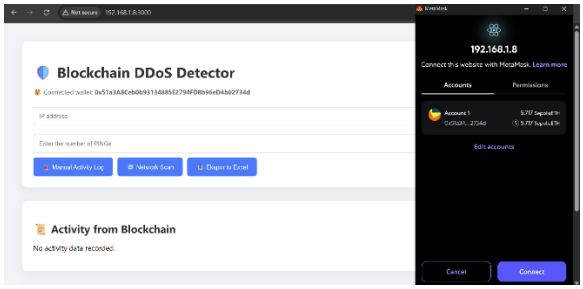
Sementara *blockchain* berfungsi sebagai penyimpanan data utama yang bersifat permanen, *MongoDB* digunakan untuk menyimpan salinan data secara lokal. Basis data ini mencatat alamat IP, waktu terjadinya serangan, status transaksi, serta durasi kejadian. Administrator selanjutnya mengolah data dari *MongoDB* menjadi laporan analitis untuk mengidentifikasi pola serangan dan mencegah terjadinya insiden serupa di masa mendatang. Arsitektur sistem aplikasi tersebut ditunjukkan pada Gambar 4.



Gambar 4. Arsitektur sistem aplikasi

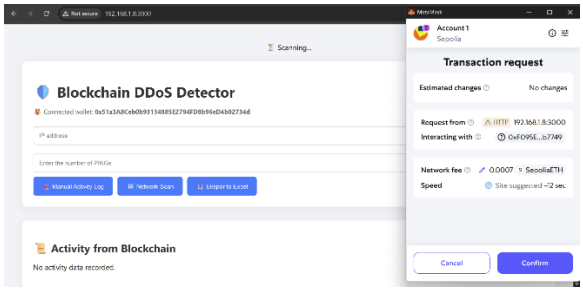
4.2. Implementasi Sistem

Tahap implementasi merupakan bagian paling krusial dalam penelitian ini. Proyek ini mencakup pengembangan dan pengujian sistem deteksi DDoS berbasis *blockchain* secara akurat. Tahap awal implementasi diawali dengan konfigurasi aplikasi, yang meliputi pembangunan sistem *backend* menggunakan bahasa pemrograman *Python* dan pustaka *Web3.py* untuk berinteraksi dengan *smart contract* yang dikembangkan dalam bahasa *Solidity*. Pada sisi *frontend*, *React.js* digunakan untuk membangun antarmuka pengguna yang memungkinkan administrator memantau serta berinteraksi dengan sistem secara *real-time*. Aplikasi kemudian terhubung dengan *MetaMask* yang berperan sebagai perantara antara pengguna dan jaringan *blockchain*. Sebagaimana ditunjukkan pada Gambar 5, ketika pengguna ingin mencatat alamat IP yang mencurigakan ke dalam *blockchain*, *MetaMask* akan meminta proses autentikasi dan selanjutnya memberikan otorisasi terhadap transaksi tersebut.



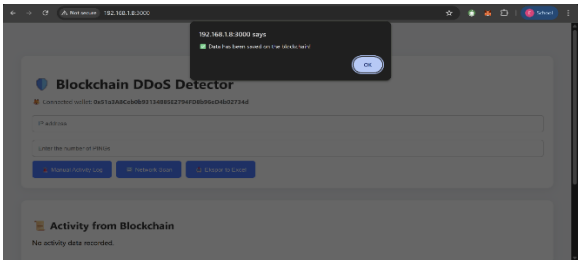
Gambar 5. Koneksi *e-wallet metamask*

Setelah terhubung dengan *MetaMask*, administrator dapat memulai proses pemindaian jaringan (*IP scan*) untuk mendeteksi indikasi potensi serangan DDoS. Pengujian aplikasi dilakukan dengan mensimulasikan serangan DDoS melalui pengiriman permintaan dalam jumlah besar ke sistem. Modul pendeteksi DDoS kemudian mengidentifikasi lonjakan permintaan yang signifikan dari satu atau beberapa alamat IP dan mengkategorikannya sebagai aktivitas mencurigakan. Selanjutnya, *smart contract* mengambil alamat IP tersebut dan mencatatnya ke dalam *blockchain Ethereum* sebagai transaksi yang bersifat tidak dapat diubah (*immutable*). Prosedur verifikasi *MetaMask* tersebut ditunjukkan pada Gambar 6.



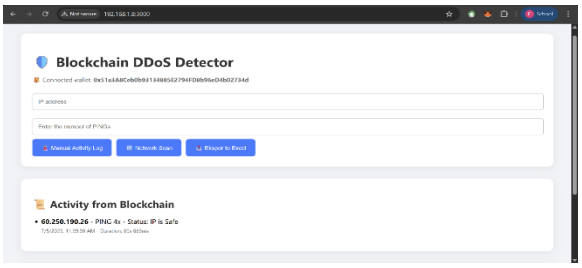
Gambar 6. Verifikasi transaksi *metamask*

Setelah proses verifikasi melalui *MetaMask* selesai, sistem akan memulai pencarian terhadap lonjakan *PING* yang berkaitan dengan alamat IP yang mencoba mengakses jaringan. Pada tahap ini, sistem menganalisis pola lalu lintas untuk mengidentifikasi aktivitas yang tidak wajar. Sebagaimana ditunjukkan pada Gambar 7, setelah proses pemindaian selesai, akan muncul notifikasi yang menyatakan bahwa data telah berhasil dicatat secara benar pada jaringan blockchain.



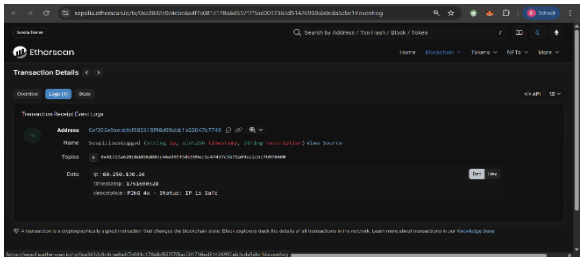
Gambar 7. Data tersimpan pada jaringan blockchain

Administrator dapat melihat status deteksi melalui antarmuka sistem yang menampilkan informasi seperti status koneksi *wallet*, alamat IP, jumlah *PING*, *timestamp*, durasi, serta tautan menuju *Etherscan*. *Etherscan Blockchain Explorer* memungkinkan hasil transaksi dapat langsung terlihat secara publik. Layanan ini menyajikan informasi rinci mengenai setiap transaksi, termasuk alamat IP, deskripsi kejadian, jumlah *PING*, waktu pencatatan, alamat *wallet*, serta isi data yang tersimpan. Sistem *Blockchain DDoS Detector* menampilkan seluruh aktivitas yang telah terdokumentasi, sebagaimana ditunjukkan pada Gambar 8.

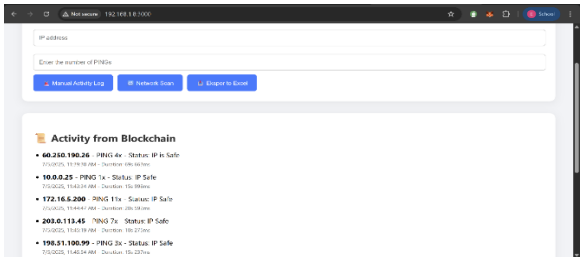


Gambar 8. Aktivitas deteksi serangan DDoS

Hasil pengujian menunjukkan bahwa sistem yang dibangun mampu memantau aktivitas jaringan, mendokumentasikannya secara otomatis pada *blockchain*, serta mengirimkan data tersebut dalam bentuk yang dapat diverifikasi. Gambar 9 memperlihatkan *transaction log* yang tersimpan pada jaringan blockchain. Pada tahap pengujian berikutnya, dilakukan lima kali proses pemindaian dan tidak ditemukan indikasi serangan DDoS maupun alamat IP yang melakukan ping secara berlebihan terhadap sistem. Hasil pengujian tersebut ditunjukkan pada Gambar 10.

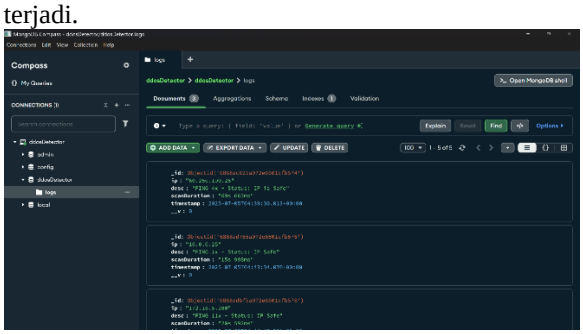


Gambar 9. Detail transaksi pada jaringan blockchain



Gambar 10. Hasil scan jaringan sistem

Gambar 11 menunjukkan bahwa data secara otomatis tersimpan dalam *database* lokal *MongoDB*. Data tersebut berfungsi sebagai sumber informasi administratif yang dapat dimanfaatkan oleh administrator di masa mendatang untuk melakukan analisis serta mitigasi terhadap permasalahan yang terjadi.



Gambar 11. Data tersimpan database mongodb

Evaluasi terhadap efektivitas sistem blockchain dalam mendeteksi serangan DDoS dilakukan dengan menyajikan data aktivitas pada Tabel 1. Selanjutnya, Tabel 2 menampilkan rincian transaksi yang terjadi pada jaringan *blockchain*.

Tabel 1. Data *Aktivitas Scan Jaringan*

IP	Deskripsi	Tanggal dan Waktu (WIB)	Durasi
60.250.190.26	PING 4x - Status: IP is Safe	7/5/2025, 11:39:30 AM	69s 663ms
10.0.0.25	PING 1x - Status: IP Safe	7/5/2025, 11:43:34 AM	15s 998ms
172.16.5.200	PING 11x - Status: IP Safe	7/5/2025, 11:44:47 AM	20s 592ms
203.0.113.45	PING 7x - Status: IP Safe	7/5/2025, 11:45:19 AM	10s 275ms
198.51.100.99	PING 3x - Status: IP Safe	7/5/2025, 11:45:54 AM	15s 237ms

Tabel 2. Transaksi Pada Jaringan *Blockchain*

Transaksi Hash	Status	Metode	Nomor Blok	Tanggal dan Waktu (UTC)	Dari (E-Wallet)	Ke (Smart Contract)
0xa383…	Success	Log Suspicious	8695288	05/07/2025 04:38:48	0x51a3…	0xF095…
0x85b6…	Success	Log Suspicious	8695311	05/07/2025 04:43:24	0x51a3…	0xF095…
0xb3c6…	Success	Log Suspicious	8695315	05/07/2025 04:44:12	0x51a3…	0xF095…
0xbee7…	Success	Log Suspicious	8695320	05/07/2025 04:45:12	0x51a3…	0xF095…
0x91d3…	Success	Log Suspicious	8695323	05/07/2025 04:45:48	0x51a3…	0xF095…

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa teknologi *blockchain* dapat diterapkan secara efektif dalam sistem keamanan jaringan untuk mendeteksi dan mencatat aktivitas yang berpotensi sebagai serangan DDoS. Integrasi antara *frontend*, *backend*, dan *blockchain* menghasilkan sistem yang mampu memantau jaringan secara *real-time*, menyimpan data secara aman dan tidak dapat diubah (*immutable*), serta menyediakan informasi yang transparan untuk analisis dan mitigasi ancaman. Dengan demikian, pendekatan berbasis *blockchain* memiliki potensi besar sebagai solusi keamanan siber yang andal, transparan, dan berkelanjutan. Sebagai saran, penelitian selanjutnya dapat mengembangkan sistem dengan skala jaringan yang lebih besar dan skenario serangan yang lebih kompleks agar performa dan skalabilitas dapat diuji secara lebih komprehensif. Selain itu, integrasi dengan metode kecerdasan buatan atau *machine learning* dapat dipertimbangkan untuk meningkatkan akurasi deteksi serta mempercepat respons terhadap ancaman siber yang semakin berkembang.

DAFTAR PUSTAKA

[1] S. Fallah and A. J. Bidgoly, "B Enchmarking M Achine L Earning a Lgorithms," *Jordanian J. Comput. Inf. Technol.*, vol. 05, no. 03, pp. 216–230, 2019.

[2] M. Das and Z. Wang, "Ed25519: a New Secure Compatible Elliptic Curve for Mobile Wireless Network Security," *Jordanian J. Comput. Inf. Technol.*, vol. 8, no. 1, pp. 57–71, 2022, doi: 10.5455/jjcit.71-1636268309.

[3] B. Irawan and A. R. Ardiyanto, "Jurnal Informatika : Jurnal pengembangan IT Design and Implementation of IoT-Based Smart Election Using ESP32 and RFID," vol. 10, no. 3, pp. 727–738, 2025, doi: 10.30591/jpit.v10i3.8412.

[4] S. Wani, M. Imthiyas, H. Almohamedh, K. M. Alhamed, S. Almotairi, and Y. Gulzar, "Distributed denial of service (Ddos) mitigation using blockchain—a comprehensive insight," *Symmetry (Basel).*, vol. 13, no. 2, pp. 1–21, 2021, doi: 10.3390/sym13020227.

[5] V. K. Singh, D. Sivashankar, K. Kundan, and S. Kumari, "An Efficient Intrusion Detection and Prevention System for DDOS Attack in WSN Using SS-LSACNN and TCSLR," *J. Cyber Secur. Mobil.*, vol. 13, no. 1, pp. 135–159, 2024, doi: 10.13052/jcsm2245-1439.1315.

[6] O. I. Falowo, S. Popoola, J. Riep, V. A. Adewopo, and J. Koch, "Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents," *IEEE Access*, vol. 10, pp. 134038–134051, 2022, doi: 10.1109/ACCESS.2022.3231847.

[7] M. Lehto, "Cyber-Attacks Against Critical Infrastructure BT - Cyber Security: Critical Infrastructure Protection," M. Lehto and P. Neittaanmäki, Eds., Cham: Springer International Publishing, 2022, pp. 3–42. doi: 10.1007/978-3-030-91293-2_1.

[8] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review," *Soft Comput.*, vol. 27, no. 18, pp. 13039–13075, 2023, doi: 10.1007/s00500-021-06608-1.

[9] D. Tymoshchuk, O. Yasniy, M. Mytnyk, N. Zagorodna, and V. Tymoshchuk, "Detection and classification of DDoS flooding attacks by machine learning method," *CEUR Workshop Proc.*, vol. 3842, pp. 184–195, 2024.

[10] B. M. Amro, S. Salah, and M. Moreb, "A Comprehensive Architectural Framework of Moving Target Defenses Against DDoS Attacks," *J. Cyber Secur. Mobil.*, vol. 12, no. 4, pp. 605–627, 2023, doi: 10.13052/jcsm2245-1439.1248.

[11] H. Mateen and M. Shahzad, "Factors Effecting Businesses due to Distributed Denial of Service (DDoS) Attack," in *2021 International Conference on Innovative Computing (ICIC)*, 2021, pp. 1–7. doi: 10.1109/ICIC53490.2021.9692965.

[12] M. K. Sinha, N. Sahu, R. Pandey, S. Shukla, M. Chahar, and R. Tiwari, "Investigation of DDoS attacks in Network Intrusion Detection System Using ML Approach," in *2024 International Conference on Advances in Computing, Communication and Materials (ICACCM)*, 2024, pp. 1–6. doi: 10.1109/ICACCM61117.2024.11059231.

[13] E. K. Aprilia Tobing, R. E. Septya, and Y. Servanda, "Comparative Analysis of Network Security: Firewall, IDS, and AI-Based Defense Against DDoS Attacks," *J. Artif. Intell. Eng. Appl.*, vol. 4, no. 3, pp. 1818–1822, 2025, doi: 10.59934/jaiea.v4i3.1026.

[14] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: an overview," *PeerJ Comput. Sci.*, vol. 9, pp. 1–50, 2023, doi: 10.7717/peerj-cs.1705.

[15] Y. I. Hamodi, A. A. Majeed, K. H. Jihad, and B. A. Qader, "Detect and Mitigate Blockchain-Based DDoS Attacks Using Machine Learning and Smart Contracts," *Inform.*, vol. 46, no. 7, pp. 55–62, 2022, doi: 10.31449/inf.v46i7.4033.

[16] S. Nikolić, S. Matić, D. Čapko, S. Vukmirović, and N. Nedić, "Development of a Blockchain-Based Application for Digital Certificates in Education,"

in *2022 30th Telecommunications Forum (TELFOR)*, 2022, pp. 1–4. doi: 10.1109/TELFOR56187.2022.9983672.

[17] N. Saran and N. Kesswani, "Intrusion Detection System for Internet of Medical Things Using Gru With Attention Mechanism-Based Hybrid Deep Learning Technique," *Jordanian J. Comput. Inf. Technol.*, vol. 11, no. 2, pp. 136–150, 2025, doi: 10.5455/jjcit.71-1725609265.

[18] A. Mishra, B. B. Gupta, D. Peraković, and Z. Zhou, "Defensive Approach using Blockchain Technology against Distributed Denial of Service attacks," *CEUR Workshop Proc.*, vol. 3080, 2021.

[19] Y. Liu, Y. Zhang, Z. Lin, Z. Wang, and X. Wang, "Simulation Method for Blockchain Systems with a Public Chain," *Sensors*, vol. 22, no. 24, 2022, doi: 10.3390/s22249750.

[20] A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, "AccessChain: An access control framework to protect data access in blockchain enabled supply chain," *Futur. Gener. Comput. Syst.*, vol. 148, pp. 380–394, 2023, doi: 10.1016/j.future.2023.06.009.

[21] H. Vaghela and V. Khirasaria, "A Review on Detection and Prevention of the DDoS Attacks in the Blockchain," in *2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 2023, pp. 71–75. doi: 10.1109/ICCCIS60361.2023.10425005.

[22] N. O. Komleva and O. I. Tereshchenko, "Requirements for the development of smart contracts and anoverview of smart contract vulnerabilities at the Solidity codelevel on the Ethereum platform," *Her. Adv. Inf. Technol.*, vol. 6, no. 1, pp. 54–68, 2023, doi: 10.15276/hait.06.2023.4.

[23] S. Jiang *et al.*, "BSD-Guard: A Collaborative Blockchain-Based Approach for Detection and Mitigation of SDN-Targeted DDoS Attacks," *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/1608689.

[24] J. Cheng *et al.*, "Cooperative Detection Method for DDoS Attacks Based on Blockchain," *Comput. Syst. Sci. Eng.*, vol. 43, no. 1, pp. 103–117, 2022, doi: 10.32604/csse.2022.025668.

[25] Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, "Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey," *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22031094.

[26] K. G. Arachchige, P. Branch, and J. But, "An Analysis of Blockchain-Based IoT Sensor Network Distributed Denial of Service Attacks," *Sensors*, vol. 24, no. 10, 2024, doi: 10.3390/s24103083.

[27] X. Liu, Z. Huang, Q. Wang, Y. Chen, and Y. Cao, "A Repeated Game-Based Distributed Denial of Service Attacks Mitigation Method for Mining Pools," *Electron.*, vol. 13, no. 2, pp. 1–31, 2024, doi: 10.3390/electronics13020398.

[28] X. Liu, Z. Huang, Q. Wang, X. Jiang, Y. Chen, and B. Wan, "Analyzing Miners' Dynamic Equilibrium in Blockchain Networks under DDoS Attacks," *Electron.*, vol. 12, no. 18, pp. 1–27, 2023, doi: 10.3390/electronics12183903.

[29] R. Jmal, W. Ghabri, R. Guesmi, B. M. Alshammari, A. S. Alshammari, and H. Alsaif, "Distributed Blockchain-SDN Secure IoT System Based on ANN to Mitigate DDoS Attacks," *Appl. Sci.*, vol. 13, no. 8, 2023, doi: 10.3390/app13084953.

[30] A. F. Bahari and A. Pramudwiatmoko, "Implementation of Rapid Application Development (RAD) Method for Mobile-Based Ice Cream Ordering Application," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 5, no. 1, pp. 283–291, 2024, doi: 10.57152/malcom.v5i1.1747.

[31] B. Irawan, M. Wahyu Sabiqudin, N. Anwar, and B. Tjahjono, "Leveraging Blockchain-based Smart Contracts to Develope Trustworthy Customer Agreements," *Int. J. Sci. Technol. Manag.*, vol. 4, no. 4, pp. 1081–1089, 2023, doi: 10.46729/ijstm.v4i4.907.

[32] M. Kumar, "Designing resilient front end architectures for real-time web application UI developer," no. 08, pp. 229–240, 2024.

[33] Y. Zanevych, "Flask Vs. Django Vs. Spring Boot: Navigating Framework Choices for Machine Learning Object Detection Projects," pp. 311–318, 2024, doi: 10.36074/logos-29.03.2024.066.

[34] Q. Wang, R. Li, Q. Wang, S. Chen, M. Ryan, and T. Hardjono, "Exploring Web3 From the View of Blockchain," vol. 2, pp. 1–38, 2022, [Online]. Available: http://arxiv.org/abs/2206.08821

[35] Bambang Irawan, "Blockchain Technology as an Alternative Method of Payment Transaction Proof," *Int. J. Sci. Technol. Manag.*, vol. 2, no. 5, pp. 1769–1774, 2021, doi: 10.46729/ijstm.v2i5.309.

[36] 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: 10.46729/ijstm.v5i2.1084.

[37] R. Toorajipour, P. Oghazi, V. Sohrabpour, P. C. Patel, and R. Mostaghel, "Block by block: A blockchain-based peer-to-peer business transaction for international trade," *Technol. Forecast. Soc. Change*, vol. 180, p. 121714, 2022, doi: https://doi.org/10.1016/j.techfore.2022.121714.

[38] C. Xu *et al.*, "A Federated Learning Architecture for Blockchain DDoS Attacks Detection," *IEEE Trans. Serv. Comput.*, vol. 17, no. 5, pp. 1911–1923, 2024, doi: 10.1109/TSC.2024.3453764.

[39] Osato Itohan Oriekhoe, Oluwaseun Peter Oyeyemi, Binaebi Gloria Bello, Ganiyu Bolawale Omotoye, Andrew Ifesinachi Daraojimba, and Adedayo Adefemi, "Blockchain in supply chain management: A review of efficiency, transparency, and innovation," *Int. J. Sci. Res. Arch.*, vol. 11, no. 1, pp. 173–181, 2024, doi: 10.30574/ijsra.2024.11.1.0028.