Pengembangan Keamanan Sistem Rekam Medis Berbasis Blockchain dengan Smart Contract

Purwono Purwono[1], Pramesti Dewi[2], Safar Dwi Kurniawan*[3]
[1]Program Studi Informatika, Universitas Harapan Bangsa, Purwokerto
[2]Program Studi S1 Keperawatan, Universitas Harapan Bangsa, Purwokerto
[3]Program Studi D3 Teknik Komputer, Politeknik Harapan Bersama, Tegal
E-mail: [1]purwono@uhb.ac.id , [2]pramestidewi@uhb.ac.id, *[3]**safar.kurniawan45@gmail.com**

Abstrak

Manipulasi data kesehatan memicu keresahan masyarakat dan menurunkan tingkat kepercayaan terhadap langkah antisipatif yang dilakukan pemerintah Indonesia. Teknologi Blockchain menjadi salah satu solusi untuk mencegah data kesehatan yang berpotensi untuk dimanipulasi. Smart contract adalah protokol yang berjalan di jaringan blockchain. Metode ini mengikat suatu kesepakatan antara beberapa pihak dalam suatu perjanjian. Data kesehatan ini dapat dilindungi dari pihak internal dengan membuat kontrak cerdas antara dokter, pasien, dan pengelola website. Data diagnosis yang dibuat oleh dokter baru adalah valid jika pasien setuju. Administrator hanya dapat mengakses data jika disetujui oleh dokter dan pasien. Pengujian keamanan dilakukan melalui serangan injeksi SQL. Sistem yang belum menerapkan kontrak pintar dapat dikompromikan melalui uji injeksi muatan, sedangkan sistem yang telah menerapkan kontrak pintar hanya dapat memecahkan kueri login. Pengujian manipulasi data 10 kali setelah login berhasil menunjukkan bahwa data yang telah disimpan tidak dapat diubah karena memerlukan kontrak pintar.

Kata Kunci*— kesehatan, smart contract, keamanan, sql injections, sistem rekam medis*

1. PENDAHULUAN

Seiring dengan semakin berkembangnya teknologi, ancaman *cyber* terhadap komputer juga semakin meningkat [1]. Salah satu ancaman tersebut adalah percobaan manipulasi data pada suatu sistem informasi. Manipulasi data kasus rekam medis sudah menjadi berita yang sering kita dengar di berbagai media baik konvensional maupun online. Lonjakan statistik orang yang terkena dampak Covid-19 dianggap data yang dimanipulasi karena peningkatan pasien yang terlalu cepat dan tidak wajar. Manipulasi ini telah terjadi di berbagai negara seperti China, Amerika Serikat, Rusia, dan Turki [2]. Hal ini menimbulkan ketidakpercayaan dari berbagai kalangan masyarakat di Indonesia terhadap Rumah Sakit dan RS Pemerintah. Kekhawatiran yang terjadi di masyarakat semakin meluas dengan adanya pemberitaan tentang berita palsu oleh pihak-pihak yang tidak bertanggung jawab.

Manipulasi data Covid-19 pada EHR (*Electronic Health Record*) di sebuah rumah sakit bisa saja terjadi akibat ulah oknum yang tidak bertanggung jawab [4] dan tentunya sangat merugikan banyak pihak. Upaya manipulasi data ini bisa terjadi kapanpun dan dimanapun sehingga data bersifat manipulatif dan tidak bisa dipertanggungjawabkan. Terdapat berbagai jenis upaya manipulasi data dengan berbagai serangan pada sistem informasi yang berbahaya khususnya pada data pribadi.

Jenis serangan yang paling umum pada sistem adalah *SQL Injection* untuk mencuri informasi atau tujuan tertentu [7]. *SQL Injection* adalah salah satu jenis serangan yang paling umum pada sistem berbasis web [8]. EHR berbasis web dengan data sensitif dan pribadi memiliki peluang tinggi untuk dicuri atau dimanipulasi. Salah satu solusi untuk melindungi data dari

serangan jenis ini dapat memanfaatkan teknologi *Blockchain* yaitu teknologi untuk mencatat transaksi antara beberapa pihak secara efisien dan dapat diverifikasi serta bersifat permanen menggunakan konsep *distributed ledger* [9] untuk komputasi yang aman [10] dalam jaringan *peer to peer* [11]. Perlindungan data EHR dengan teknologi *blockchain* telah dilakukan oleh beberapa peneliti sebelumnya seperti Sharma [12] yang menyatakan bahwa teknologi dapat mengamankan data EHR dari pihak yang tidak berhak. Penelitian terkait juga dilakukan oleh Safna [13] menyatakan bahwa *blockchain* dapat melacak dan mengantisipasi serangan terhadap data EHR. Penelitian yang dilakukan oleh Kim [14] menyimpulkan bahwa *blockchain* dapat menjadi sistem keamanan pada data EHR dan dianggap lebih efisien. Penelitian Li menghasilkan sebuah sistem yang dapat memberikan keamanan privasi data untuk EHR dengan memanfaatkan teknologi *blockchain* [15].

Data EHR yang difokuskan untuk dilindungi dalam penelitian ini adalah yang terkait dengan Covid-19. Penambahan data pada rekam medis akan diverifikasi menggunakan metode *smart contract* atau kontrak pintar. Metode ini merupakan kesepakatan antara dua orang atau lebih dalam bentuk kode komputer. Kontrak pintar berjalan di jaringan *Blockchain* [16], sehingga kesepakatan difasilitasi, dieksekusi, dan ditegakkan di jaringan ini [17]. Upaya perlindungan data rekam medis dengan metode *smart contract* diharapkan dapat meningkatkan kepercayaan masyarakat terhadap rumah sakit dan pemerintah karena adanya jaminan data yang dianggap aman sehingga kecemasan dapat mereda, dan masyarakat lebih patuh terhadap protokol kesehatan.

Kontrak pintar akan mengikat kesepakatan antara pasien, rumah sakit (dokter), dan administrator EHR mengenai keaslian data rekam medis. Masing-masing anggota melakukan konsensus bersama yaitu memvalidasi semua data dan hanya mengakui data mayoritas yang disetujui sebagai data yang benar [18], sehingga ketika salah satu rekam medis berbeda, data tersebut akan dianggap data rusak atau dimanipulasi dan akan diabaikan oleh anggota.

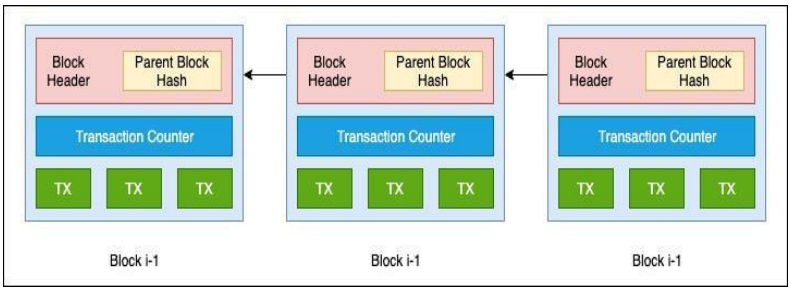
Kontrak pintar dianggap sebagai solusi yang tepat untuk menangani masalah manipulasi data Covid-19. Data diagnosa Covid-19 yang ditambahkan oleh dokter ke dalam SIMRS akan diverifikasi dan disimpan dalam *database* jika semua pihak terkait telah menyetujuinya, demikian juga jika ada perubahan data salah satu pasien yang dilakukan oleh *website administrator*. Orang yang tidak bertanggung jawab yang mencoba mengubah data Covid-19 dengan niat buruk tidak dapat melakukan tindakan tersebut karena membutuhkan kunci validasi pribadi dari setiap anggota Blockchain. Covid-19 data aman dan dapat dilaporkan dengan benar di situs resmi Pemerintah Republik Indonesia.

2. METODE PENELITIAN

2.1. Arsitektur Blockchain

Blockchain didistribusikan menggunakan skema konsensus yang memungkinkan data transaksi disimpan dengan aman di jaringan *Blockchain* setelah melalui proses verifikasi dan validasi tanpa intervensi pihak ketiga [11]. Semua data transaksi akan terekam di semua jaringan *Blockchain*, dan tentunya hal ini tidak terpusat pada satu pihak saja. Teknologi ini akan mencatat

semua transaksi di setiap node sehingga sulit untuk dimodifikasi oleh orang yang tidak bertanggung jawab [19]. Gambar 1 mengilustrasikan contoh implementasi *Blockchain*. Dengan hash blok sebelumnya yang terdapat di *header* blok, sebuah blok hanya memiliki satu blok permanen. Blok pertama dari blockchain disebut sebagai blok genesis, yang tidak memiliki blok induk [9].



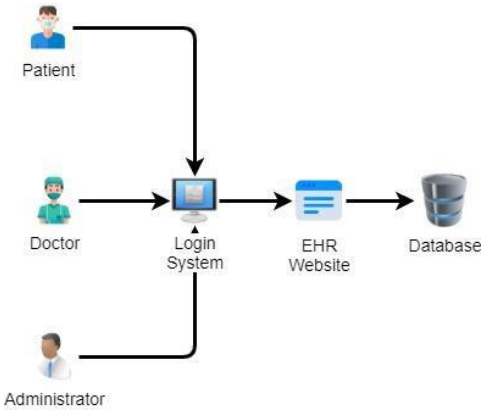
Gambar 1. Rantai Blockchain

Algoritma konsensus adalah protokol yang digunakan untuk mencapai kesepakatan pada satu nilai data. Algoritma konsensus bersifat mekanistik dan secara otomatis menyinkronkan semua data transaksi di *Blockchain* [20]. Mekanisme algoritme ini pertama-tama memerlukan kepastian keadaan jaringan dan penentuan *node* mana yang dapat memvalidasi transaksi. Salah satu algoritme konsensus yang tersedia adalah *proof-of-work* (PoW), yang membutuhkan penyelesaian matematika rumit dalam kriptografi melalui *node* pada jaringan untuk berjalan bersama dan proses acak memberikan jawaban atas eksperimen dan kesalahan dasar. [21]. *Proof of work* juga bisa disebut proses *mining* karena komputer modern dapat melakukan transaksi dengan cepat, kita dapat kesulitan dalam memecahkan blok hash [22]. Dapat dengan mudah disimpulkan bahwa algoritma ini menghasilkan keputusan mayoritas dalam suatu kelompok. Keputusan mayoritas ini harus diterima oleh semua anggotanya. Anggota yang tidak setuju dengan keputusan mayoritas dianggap bukan anggota lagi. Implementasi nyata dalam menyelaraskan data transaksi di jaringan *blockchain* adalah ketika salah satu data transaksi berbeda dengan mayoritas data jaringan, maka dianggap sebagai data yang tidak valid atau tidak valid. Ini membuat keamanan yang sangat baik dalam melindungi data semua anggota.

2.2. Blockchain Sebagai Solusi Keamanan Data Rekam Medis

Data kesehatan pribadi merupakan data vital dan memberikan nilai tinggi untuk pengembangan sistem perawatan kesehatan yang lebih baik [23]. EHR yang berjalan saat ini adalah sistem informasi berbasis website, dan hanya orang-orang tertentu yang berkepentingan saja yang dapat mengaksesnya [24]. Pasien tidak memiliki kontrol akses untuk menyetujui atau menolak data diagnostik dokter yang disimpan dalam sistem EHR. *Administrator* situs web juga dapat dengan mudah memanipulasi data diagnostik tanpa persetujuan pasien dan dokter. Manipulasi ini juga bisa terjadi oleh elemen internal karena datanya terpusat. Gambar 2 adalah gambaran dari sistem EHR saat ini.

Upaya memanipulasi data diagnostik juga dapat berasal dari serangan luar. Kerentanan sistem berbasis website dari serangan *SQL Injection* membuat data sensitif seperti Covid-19 harus dijaga ketat. Data yang ditransaksikan pada *blockchain* tidak memiliki otoritas pusat sehingga data tersebut dipertahankan dan dikonfirmasi oleh semua jaringan *peer to peer* [25]. Ini adalah salah satu cara agar data Covid-19 bisa terlindung. Semua jaringan *peer* di *blockchain* harus mengonfirmasi setiap penambahan data baru ke sistem EHR. Data yang ditambahkan tersebut kemudian menjadi data yang benar-benar valid dan aman karena telah lolos persetujuan semua anggota jaringan. Serangan data EHR dengan *SQL Injection* dapat diantisipasi karena *blockchain* akan mencegah perubahan data atau penambahan data baru oleh pihak selain anggota jaringan.



Gambar 2. Gambaran Alur Sistem Informasi Rekam Medis

2.3. Alur Proses Penelitian

Alur proses transaksi *blockchain* yang diusulkan dapat digambarkan dalam empat tahap utama untuk melindungi data covid-19 dari serangan injeksi SQL. Empat tahap tersebut adalah sebagai berikut:

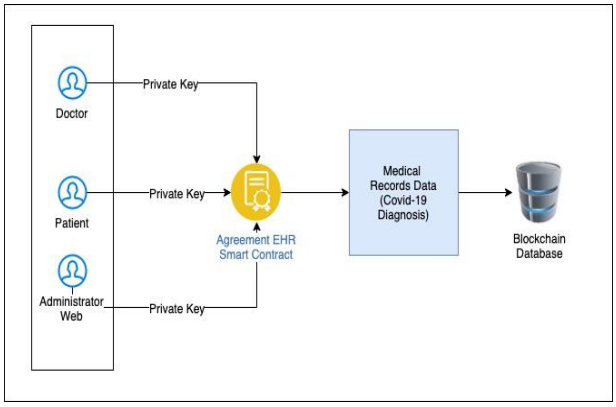
1. Rumah sakit yaitu dokter, pasien, administrator sistem EHR membuat *smart contract* sebagai hak akses data pasien Covid-19.
2. Pihak rumah sakit pada saat melakukan transaksi data baru yaitu dokter yang membuat rekam diagnosis Covid-19 ke dalam sistem EHR terlebih dahulu akan diotentikasi dengan *smart contract*.
3. Pasien melakukan verifikasi berupa persetujuan atau penolakan diagnosis Covid-19 yang dibuat oleh dokter.
4. Perubahan data pasien juga harus diverifikasi oleh pasien.

Langkah pertama dalam proses penandatanganan *smart contract* adalah mengikat perjanjian anggota *blockchain*. *Smart contract* dapat dibuat menggunakan bahasa pemrograman *solidity ehereum blockchain* [26]. Anggota hanya dapat ditambahkan ke jaringan *blockchain*

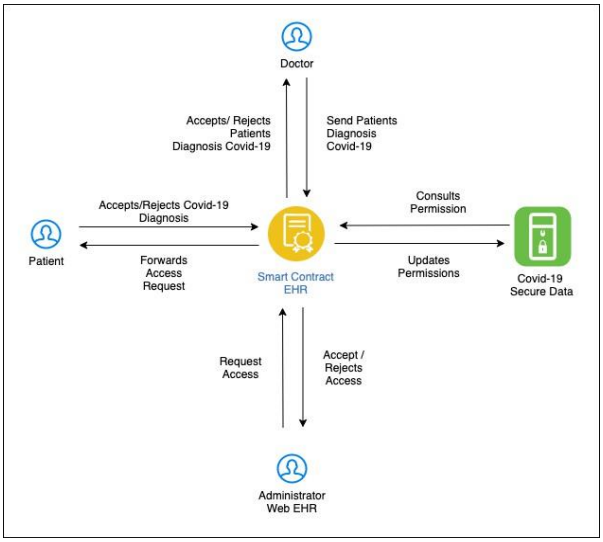
P-ISSN: 2089-676X
E-ISSN: 2549-0796

ethereum jika mereka memiliki kunci pribadi atau *private key* [27]. *Private key* ini bisa dimiliki jika kita sudah memiliki akun *ethereum*. Tahapan ini dapat dilihat pada Gambar 3.

Berdasarkan Gambar 3, semua anggota jaringan yaitu dokter, pasien, dan administrator EHR terlebih dahulu harus menandatangani *smart contract* untuk masuk ke database EHR. Hak akses seluruh anggota jaringan *blockchain* dalam proses transaksi data diagnosa Covid-19 harus melalui tahap verifikasi approval dengan *smart contract* dan dapat dilihat pada Gambar 4. Dokter hanya dapat mengirimkan data diagnosa Covid-19 jika telah menandatangani akta kontrak pintar. Data diagnostik yang dikirim tidak dapat langsung valid sampai pasien benar-benar menerima penerimaan. Administrator web EHR hanya dapat mengakses dan mengubah data jika pasien dan dokter telah setuju untuk mengaksesnya.



Gambar 3. Menandatangani Kontrak Cerdas

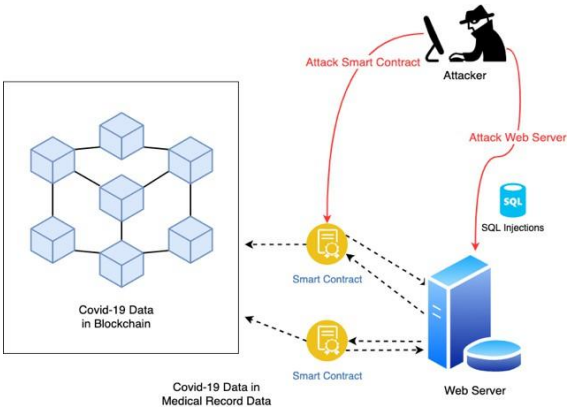


Gambar 4. Hak Akses Anggota Blockchain

P-ISSN: 2089-676X
E-ISSN: 2549-0796

2.4. Skenario Keamanan Data Rekam Medis

Keamanan data Covid-19 awalnya diamankan dari upaya manipulasi internal oleh anggota jaringan blockchain. Keamanan data ini juga harus diperhatikan dari serangan luar yang berisiko pencurian data atau manipulasi data. Sistem EHR berbasis situs web rentan terhadap jenis serangan seperti *SQL Injections*. Tahap penyerangan dengan model ini dilakukan seperti memasukkan *query* yang berbahaya seperti tautology dan *automatic coding* [28]. Skenario penyerangan ini dapat dilihat pada Gambar 5.



Gambar 5. Skenario SQL Injections

3. HASIL DAN PEMBAHASAN

Implementasi sistem keamanan data Covid-19 ini menggunakan *smart contract* yang dapat dibuat dengan menggunakan bahasa pemrograman solidity [29] milik *blockchain ethereum*.

3.1. Smart Contract

Smart contract akan mengikat perjanjian data diagnosis Covid-19 antara dokter, pasien, dan pengelola situs web. Data diagnostik meliputi nama pasien dan status pasien dengan status seperti OTG (Orang tanpa Gejala), ODP (Orang Dalam Pemantauan), PDP (Pasien Dalam Pengawasan), Positif dan Negatif [30]. Smart contract yang telah dibuat dapat dilihat pada Gambar 6 dan kode *solidity* untuk validasi data diagnosis Covid-19 dapat dilihat pada Gambar 7.

Gambar 6. Pembuatan Smart Contract

P-ISSN: 2089-676X
E-ISSN: 2549-0796

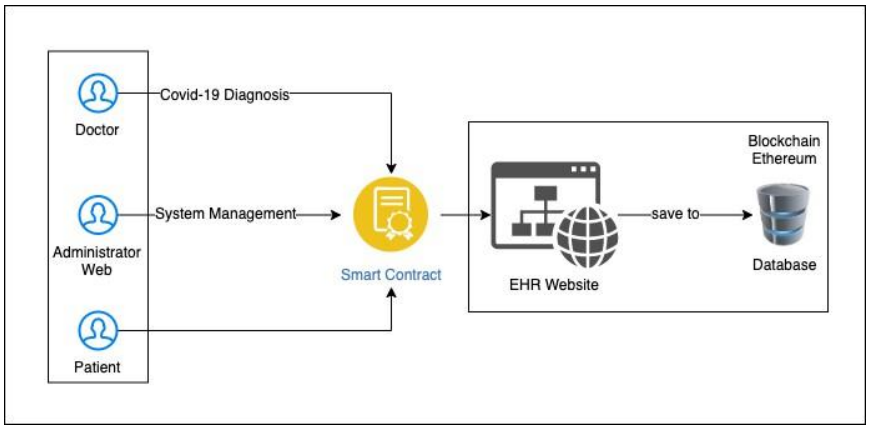
```
1   function verifyDiagnosis(uint256 _id) public payable
2   {
3       Diagnosis memory _diagnosis = diagnosis[_id];
4       address payable _doctor = _diagnosis.doctor;
5       require(_diagnosis.id > 0 && _diagnosis.id <= diagnosisCount);
6       require(!_diagnosis.verified);
7       require(_doctor != msg.sender);
8       _diagnosis.doctor = msg.sender;
9       _diagnosis.verified = true;
10      diagnosis[_id] = _diagnosis;
11      emit DiagnosisVerified(
12          diagnosisCount,
13          _diagnosis.patientName,
14          _diagnosis.patientStatus,
15          msg.sender,
16          true
17      );
18  }
```

Gambar 7. Validasi Diagnosis Covid-19 menggunakan Smart Contract

Fungsi *verifyDiagnosis()* adalah bagian dari kode untuk *smart contract* yang dibuat untuk memvalidasi apakah data diagnostik benar atau salah. Fungsi ini diperlukan untuk mencapai kesepakatan kontrak bersama. Pada baris 11 sampai 16, setelah semua pihak menyepakati data bersama, kontrak terverifikasi yang awalnya dinilai sebagai "salah" berubah menjadi "benar". Status "benar" adalah bukti bahwa diagnosis itu valid.

3.2. Analisis Implementasi dan Kegunaan

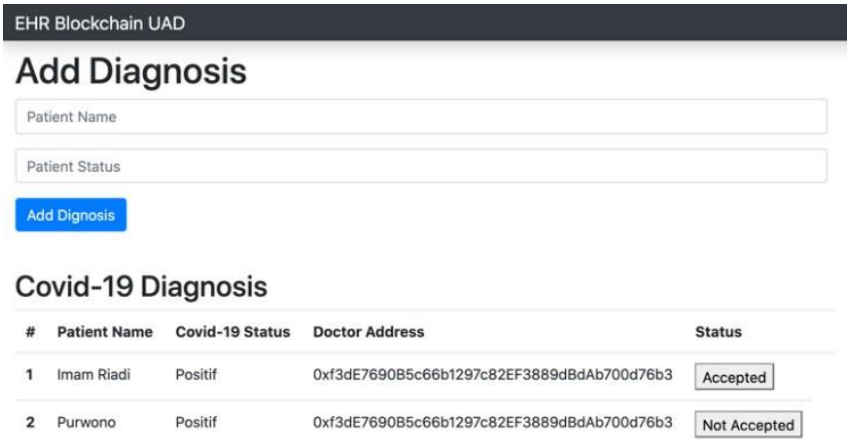
Keamanan sistem diperkuat dengan menambahkan *smart contract* untuk memvalidasi semua data diagnostik yang dibuat oleh dokter. Kontrak pintar juga memvalidasi aktivitas pemrosesan data yang dilakukan oleh administrator situs web. Gambar 8 merupakan gambaran sistem setelah diterapkan menggunakan *smart contract*.



Gambar 8. EHR dengan Smart Contract

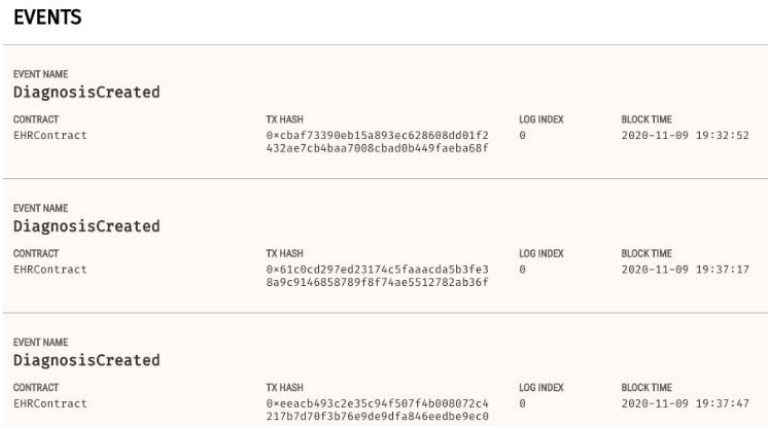
P-ISSN: 2089-676X
E-ISSN: 2549-0796

Dokter adalah anggota dari *blockchain* yang tugasnya memberikan diagnosa untuk pasien Covid-19. Data diagnostik dikirim melalui sistem berbasis situs web. Gambar 9 adalah antarmuka pengguna saat dokter menambahkan data diagnostik baru.



Gambar 9. Tampilam Penambahan Data EHR

Berdasarkan Gambar 9, semua data diagnostik yang dikirim ke sistem harus terlebih dahulu divalidasi oleh pasien. Status tidak diterima *(not accepted)* menunjukkan belum ada kesepakatan antara kedua belah pihak terkait status diagnosis Covid-19. Diagnosis valid jika pasien menyetujui data yang dibuat oleh dokter. Semua transaksi akan dimasukkan ke dalam *smart contract* di jaringan blockchain. Semua transaksi dicatat dalam blok baru, yang tidak dapat dimanipulasi oleh orang yang bukan bagian dari *smart contract*. Gambar 10 adalah transaksi untuk menambahkan data diagnostik ke jaringan *blockchain*.



Gambar 10. Penambahan Blok Transaksi

3.3. Uji Keamanan Sistem

Keamanan data di sisi internal jaringan blockchain dapat diatasi dengan proses validasi *smart contract*. Data diagnostik yang dikirim oleh dokter hanya berlaku jika pasien telah memberikan persetujuan. Data diagnostik ini hanya dapat diubah oleh administrator situs web jika dokter dan pasien memberikan persetujuan. Keamanan data juga harus diuji terhadap serangan oleh pihak ketiga yang mencoba mencuri atau memanipulasi data diagnostik. Skenario yang diterapkan adalah proses pengujian serangan menggunakan *SQL Injections*.

Upaya penyerangan dilakukan dengan menggunakan metode *SQL Injection* terhadap website EHR yang belum dikembangkan dengan *smart contract*. Pengujian terhadap 5 jenis injeksi menunjukkan bahwa sistem masih rentan terhadap serangan jenis ini. Hasil yang lebih baik ditunjukkan ketika sistem telah dikembangkan menggunakan *smart contract*. Dari lima jenis skenario serangan, hanya satu upaya permintaan login yang berhasil. Injeksi pada *query* login ini hanya pada tahap mengakses halaman input data diagnosis oleh dokter, namun *attacker* tidak dapat langsung mengubah data diagnosis Covid-19 pasien karena data tersebut juga harus divalidasi ulang oleh pasien. Hasil uji serangan dapat dilihat pada Tabel 1 dan upaya perubahan data diagnosis covid-19 pada Tabel 2. Berdasarkan Tabel 2, penyerang berusaha mengubah data pada blok transaksi diagnostik Covid-19. Tes penyerang diubah 10 kali, tetapi semua perubahan data tidak berhasil karena diblokir oleh keamanan kontrak pintar.

Tabel 1. Uji Serangan SQL Injection

Type	Payload Example	Before	Query	After
Tautology	’or ’1’=’1’;– -	Success	Login	Failed
Tautology	’-0‖’	Success	Login	Success
Order by	1’ order by 10– -	Success	GET	Failed
Union	1’ UNION select 1,@@version ,3,4,5,6,7– -	Success	Search	Failed
Union	1’ UNION select 1,table-name,3,4,5,6, 7 from diagnosis-schema.tables – -	Success	Search	Failed

Tabel 2. Upaya Perubahan Data Diagnosis Covid-19

No	Patient Address	Result
1	0xa7615889c9E1DE8702170e7CB68B1f4FFE944425	Failed
2	0xa7615889c9E1DE8702170e7CB68B1f4FFE944425	Failed
3	0xa7615889c9E1DE8702170e7CB68B1f4FFE944425	Failed
4	0xa7615889c9E1DE8702170e7CB68B1f4FFE944425	Failed
5	0xa7615889c9E1DE8702170e7CB68B1f4FFE944425	Failed
6	0x5DbC291eb034d97768f0cdC7B5F7a3BFAC154237	Failed
7	0x5DbC291eb034d97768f0cdC7B5F7a3BFAC154237	Failed
8	0x5DbC291eb034d97768f0cdC7B5F7a3BFAC154237	Failed
9	0x5DbC291eb034d97768f0cdC7B5F7a3BFAC154237	Failed
10	0x5DbC291eb034d97768f0cdC7B5F7a3BFAC154237	Failed

4. KESIMPULAN

Hasil penelitian ini menunjukan bahwa keamanan data Covid-19 dapat ditingkatkan dengan menerapkan metode *smart contract*. Data akan disimpan secara valid berdasarkan kesepakatan bersama dengan anggota jaringan blockchain. Keamanan dari serangan *SQL injection* juga dapat ditangani dengan baik. Uji coba injeksi sistem dengan 5 jenis *payload* pada *query sistem* setelah penerapan metode *smart contract* mampu menangani serangan ini dengan pengecualian *query login* yang mampu dibobol oleh penyerang. Keberhasilan penyerang membobol sistem melalui login tidak cukup untuk mengubah data transaksi yang telah tersimpan di jaringan blockchain. Hal ini terlihat dari 10 kali upaya perubahan data oleh penyerang yang belum berhasil mengubah data diagnosis Covid-19.

DAFTAR PUSTAKA

[1] L. Usman, Y. Prayudi, and I. Riadi, "Ransomware analysis based on the surface, runtime and static code method," J. Theor. Appl. Inf. Technol., vol. 95, no. 11, pp. 2426–2433, 2017.
[2] F. S. Adiguzel and A. Cansunar, "Truth or Dare ? Detecting Systematic Manipulation of COVID-19 Statistics," J. Polit. Institutions Polit. Econ., 2020.
[3] N. R. Yunus and A. Rezki, "Lock Down Enforcement Policy in Anticipation of Corona Virus Covid-19 Spread," SALAM J. Sos. dan Budaya Syar-i, vol. 7, no. 3, 2020.
[4] S. Annaka, "Political Regime and Suspected COVID-19 Death Data Manipulation *," Cambridge, 2020.
[5] D. R. Matos, M. L. Pardal, P. Adao, A. R. Silva, and M. Correia, "Securing electronic health records in the cloud," Proc. Work. Priv. by Des. Distrib. Syst. P2DS 2018, co-located with Eur. Conf. Comput. Syst. EuroSys 2018, 2018.
[6] D. Tith et al., "Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability," Healthc. Inform. Res., vol. 26, no. 1, pp. 3–12, 2020.

[7] A. Kurniawan, I. Riadi, and A. Luthfi, "Forensic analysis and prevent of cross site scripting in single victim attack using open web application security project (OWASP) framework," J. Theor. Appl. Inf. Technol., vol. 95, no. 6, pp. 1363–1371, 2017.
[8] H. Shahriar, S. North, and W.-C. Chen, "Early Detection of SQL Injection Attacks," Int. J. Netw. Secur. Its Appl., vol. 5, no. 4, pp. 53–65, 2013.
[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr.2017, no. June, pp. 557–564, 2017.
[10] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, "A survey of blockchain applications in different domains," ACM Int. Conf. Proceeding Ser., pp. 17–21, 2018.
[11] S. S. Sarmah, "Understanding Blockchain Technology," Comput. Sci. Eng., vol. 8, no. 2, pp. 23–29, 2018.
[12] Y. Sharma and B. Balamurugan, "Preserving the Privacy of Electronic Health Records using Blockchain," Procedia Comput. Sci., vol. 173, no. 2019, pp. 171–180, 2020.
[13] F. Safna, M. C. Aji, V. Mohan, S. L. Sofia, A. S. L, and A. S. P, "Securing Medical Data Using Blockchain and Cloud," Int. J. Adv. Sci. Technol., vol. 29, no. 9, pp. 3108–3114, 2020.
[14] M. Kim, S. Yu, J. Lee, Y. Park, and Y. Park, "Design of secure protocol for cloud-assisted electronic health record system using blockchain," Sensors (Switzerland), vol. 20, no. 10, pp. 1–21, 2020.
[15] L. Yue, R. N. Nortey, M. Adjeisah, P. R. Agbedanu, and X. Lui, "Blockchain Enabled Privacy Security Module for Sharing Electronic Health Records (EHRs)," Int. J. Comput. Commun. Eng., vol. 8, no. 4, pp. 155–168, 2019.
[16] S. Nzuva, "Smart Contracts Implementation, Applications, Benefits, and Limitations," Public Policy Adm. Res., vol. 9, no. 5, pp.63–75, 2019.
[17] M. Alharby and A. van Moorsel, "Blockchain Based Smart Contracts : A Systematic Mapping Study," Conf. 3rd Int. Conf. Artif. Intell. Soft Comput., no. August, pp. 125–140, 2017.
[18] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," ICOSST 2018 - 2018 Int. Conf. Open Source Syst. Technol. Proc., no. December, pp. 54–63, 2019.
[19] U. Satapathy, B. K. Mohanta, S. S. Panda, S. Sobhanayak, and D. Jena, "A Secure Framework for Communication in Internet of Things Application using Hyperledger based Blockchain," 2019 10th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2019, no. July, pp.1–7, 2019.
[20] R. P. dos Santos, "Consensus Algorithms: A Matter of Complexity?," in Blockchain Economics : Implication of Distributed Ledgers, no. June, 2019, pp. 147–170.
[21] B. Lucas and R. V. Paez, "Consensus algorithm for a private blockchain," ICEIEC 2019 - Proc. 2019 IEEE 9th Int. Conf. Electron. Inf. Emerg. Commun., no. July, pp. 264–271, 2019.

[22] A. A. G. Agung, R. G. Dillak, D. R. Suchendra, and H. Robbi, "Proof of work: Energy inefficiency and profitability," J. Theor. Appl. Inf. Technol., vol. 97, no. 5, pp. 1623–1633, 2019.
[23] X. Liang, J. Z. Li, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," IEEE 28th Annu. Int. Symp. Pers. Indoor, Mob. Radio Commun., pp. 1–5, 2017.
[24] S. M. Alkhushyni, D. M. Alzaleq, and N. L. G. Kengne, "Blockchain technology applied to electronic health records," Epic Ser. Comput., vol. 63, pp. 34–42, 2019.
[25] F. Masood and A. R. Faridi, "An Overview of Distributed Ledger Technology and its Applications," Int. J. Comput. Sci. Eng., vol. 6, no.10, pp. 422–427, 2018.
[26] A. Pinna, S. Ibba, G. Baralla, R. Tonelli, and M. Marchesi, "A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics," IEEE Access, vol. 7, no. June, pp. 78194–78213, 2019.
[27] R. Yuan, Y. Bin Xia, H. B. Chen, B. Y. Zang, and J. Xie, "ShadowEth: Private Smart Contract on Public Blockchain," J. Comput. Sci. Technol., vol. 33, no. 3, pp. 542–556, 2018.
[28] R. Alsahafi, "SQL injection attacks: Detection and prevention techniques," Int. J. Sci. Technol. Res., vol. 8, no. 1, pp. 182–185, 2019.
[29] R. M. Parizi, Amritraj, and A. Dehghantanha, "Smart contract programming languages on blockchains: An empirical evaluation of usability and security," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10974 LNCS, no. June, pp. 75–91, 2018.
[30] W. Adisasmito, Pedoman Penanganan Cepat Medis dan Kesehatam Masyarakat Covid-19 di Indonesia. 2020.