JURNAL ILMIAH FIFO **P-ISSN 2085-4315 / E-ISSN 2502-8332**
DOI: http://dx.doi.org/10.22441/fifo.2020.v12i1.007

Optimasi Keamanan Informasi Pendaftaran Event Menggunakan Teknologi Blockchain

Iqbal Busthomi[1], Imam Riadi[2], Rusydi Umar[3]

[1,3]Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan
[2]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
Jl. Prof. Dr. Soepomo, Janturan, Yogyakarta 55164
[1,2,3]iqbal1907048011@webmail.uad.ac.id, imam.riadi@is.uad.ac.id, rusydi@mti.uad.ac.id

Abstract

CV. Nyebar is an IT-based start-up that deals with event data management using a web-based application. The Event system provides account registration services as a Member and Organizer. Members of the Event System must first have an account and log-in to be able to register for the event. The process of registering events so far has not been properly secured. The event registration process will send registrant information, but the information sent has not been secured and validated first, so the Event System is still vulnerable to cyber-attacks including the registration data sniffing attack and Distributed Denial of Service (DDoS) attacks. DDoS attacks are carried out by sending messages and packet requests continuously to the business sector, hosting, social sites originating from bot at one time, resulting in overloaded network servers because of the resources (bandwidth, memory, and CPU usage) they have. the network server is used up. Blockchain which has three techniques/mechanisms including the use of hashes and proof-of-work mechanisms which can be an alternative security for event registration information because it can maintain information security, data consistency, and DDoS attacks.
Keyword: Web Application, Distributed Denial of Service (DDoS), Blockchain

Abstrak

CV. Nyebar merupakan start-up berbasis IT yang bergelut dibidang pengelolaan data event menggunakan sebuah aplikasi berbasis web. Sistem Event menyediakan layanan pendaftaran akun sebagai Member dan Organizer. Member dari Sistem Event harus memiliki akun dan log-in terlebih dahulu untuk mendaftar sebuah event. Proses pendaftaran event sejauh ini belum diamankan dengan baik. Proses pendaftaran event akan mengirimkan informasi pendaftar, namun informasi yang dikirimkan belum diamanakan dan divalidasi terlebih dahulu, sehingga Sistem Event masih rentan akan serangan siber diantaranya adalah serangan sniffing data pendaftaran dan serangan Distributed Denial of Service (DDoS). Serangan DDoS dilakukan dengan mengirimkan pesan dan permintaan paket secara terus menerus kepada sektor bisnis, hosting, situs sosial yang berasal dari bot dalam satu waktu, sehingga mengakibatkan server jaringan menjadi overload karena sumber daya (bandwith, memory, dan CPU usage) yang dimiliki server jaringan habis terpakai. Blockchain yang memiliki dua teknik/mekanisme antara lain adalah penggunaan hash dan mekanisme proof-of-work, yang dapat menjadi alternatif pengamanan informasi pemdaftaran event karena dapat menjaga keamanan informasi, kekonsistenan data, dan serangan dari DDoS.
Keyword: *Aplikasi Web, Distributed Denial of Service (DDoS), Teknologi Blockchain*

DOI: http://dx.doi.org/10.22441/fifo.2020.v12i1.007

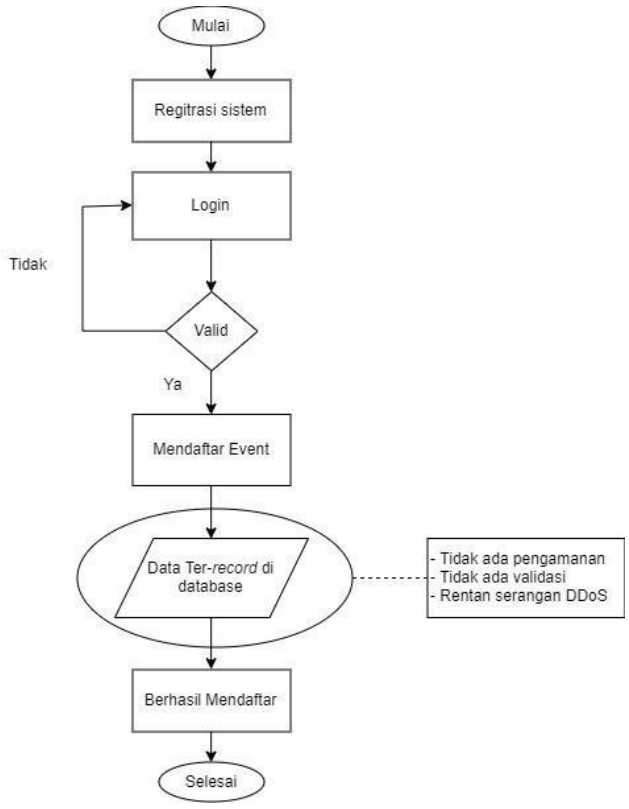
I. Pendahuluan

Perusahaan berbasis teknologi informasi berkembang dengan sangat pesat, dari perusahaan property, perusahaan finansial, hingga perusahaan IT yang bergelut dibidang pengelolaan data event. CV. Nyebar merupakan salah satu start-up atau perusahaan yang menggunakan sebuah aplikasi berbasis web yang dijadikan sebagai wadah utama untuk mengelola data-data event, baik dari segi registrasi akun, pendaftaran event,

registrasi ualng, pembayaran, hingga feedback dari penyelenggaraan event tersebut. Aplikasi yang dikelola oleh CV. Nyebar disebut dengan Sistem Event.

Sistem Event menyediakan layanan pendaftaran akun sebagai Member dan Organizer. Organizer merupakan sebuah lembaga baik profit maupun non-profit yang menyelenggarakan sebuah event, sehingga dimana akun ini memiliki privilege mempublikasikan event di Sistem Event, mengelola data pendaftaran, dan mengelola data feedback dari Member, sedangkan Member merupakan akun milik perorangan yang digunakan untuk mendaftarkan diri pada event-event yang tersedia.

Member dari Sistem Event harus memiliki akun dan log-in terlebih dahulu untuk dapat melakukan pendaftaran event. Proses pendaftaran event, seperti yang tertampil pada Gambar 1, sejauh ini belum diamankan dengan baik, karena belum diberlakukanya pengamanan, sehingga data-data yang di-record dalam proses pendaftaran event masih rentan akan kebocoran dan pengubahan data yang nantinya akan berdampak pada penyalahgunaan data-data tersebut.



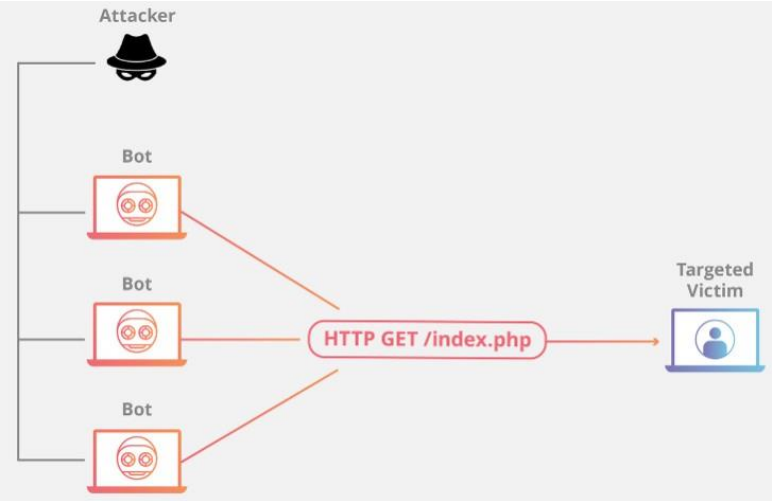
Gambar 1. *Flowchart* Proses Pendaftaran Event

Gambar 1 memaparkan proses pendaftaran event seorang Member. Proses pendaftaran event dimulai dengan member melakukan registrasi sistem untuk mendapatkan *username* dan password, keamanan data dapat ditingkatkan dengan password dan pengaturan hak. Member yang telah memiliki *username* dan password melakukan *log-in* ke Sistem Event. Member yang berhasil melakukan *log-in* akan mendapatkan *privilege* untuk melakukan pendaftaran pada sebuah event yang ada pada Sistem Event. Proses pendaftaran saat ini belum diimplementasikan keamanan sehingga informasi pendaftaran yang ter-*record* dan tersimpan dalam basisdata masih rentan akan serangan.

DOI: http://dx.doi.org/10.22441/fifo.2020.v12i1.007

Pengamanan proses pendaftaran event tidak cukup hanya dengan melakukan penyandian atau proses enkripsi-dekripsi saja, karena proses pendaftaran merupakan proses request secara terus menerus sehingga rentan akan *flooding packet request* yang menyebabkan Sistem Event menjadi tidak berfungsi secara maksimal [1]. *Distributed Denial of Service* (DDoS) adalah jenis serangan jaringan yang meningkat secara signifikan dalam beberapa tahun terakhir [2], [3].

Serangan DDoS serangan yang menimbulkan kerugian yang tinggi dan membutuhkan biaya pemulihan yang sangat besar [4]. Serangan DDoS dilakukan dengan mengirimkan pesan dan permintaan paket secara terus menerus kepada sektor bisnis, *hosting*, situs sosial yang berasal dari *host slave* atau *bot* dalam satu waktu seperti yang tertera pada Gambar 2, sehingga mengakibatkan *server* jaringan menjadi *overload* karena sumber daya (*bandwith*, *memory*, dan CPU *usage*) yang dimiliki *server* jaringan dari korban yang ditargetkan habis terpakai sehingga membuat sistem menjadi *down* [5], [6], [7], [8], [9].



Gambar 2. Visualisasi Serangan DDoS

Teknologi Blockchain dapat digunakan untuk menjamin kemanan dari sebuah informasi [10]. Konsep teknologi Blockchain sama seperti konsep yang digunakan pada basisdata terdistribusi [11]. Konsep basisdata terdistribusi adalah ketika ada data atau informasi yang tercatat maka data tersebut akan disimpan dan didistribusikan kepada setiap anggota yang tegabung pada jaringan tersebut [12]. Blockchain merupakan sebuah kumpulan blok yang membentuk rantai. Setiap blok memiliki 3 elemen yaitu data, nilai *hash* dari blok, dan nilai *hash* dari blok sebelumnya. Teknik memanfaatkan *hash* inilah yang membuat Blockchain menjadi lebih aman, karena jika ada yang mengubah salah satu blok dalam rantai blok maka nilai *hash*nya akan berubah dan blok berikutnya akan menjadi tidak valid lagi karena tidak menyimpan nilai *hash* yang valid dari blok sebelumnya. Artinya, perubahan yang dilakukan terhadap sebuah blok akan mengakibatkan seluruh rantai blok menjadi tidak valid [13].

Teknologi Blockchain yang dibangun bertujuan untuk memecahkan permasalahan pembelanjaan ganda dan verifikasi transaksi secara langsung tanpa otoritas pusat. Teknologi ini juga mampu mencegah adanya perubahan atau pemalsuan transaksi sehingga dapat digunakan untuk melakukan transaksi secara langsung secara aman. Sistem pencatatan log yang terdistribusi dan transparan dari teknologi ini dapat menjadi solusi untuk diterapkan pada pencatatan transaksi sehingga dapat menjadi upaya untuk meminimalisir tingkat kecurangan penyalahgunaan data [14].

Berdasarkan kerentanan yang diulas diatas dapat disimpulkan bahwa Sistem Event memerlukan langkah pengamanan pada proses pendaftaran event, karena dengan adanya kerentanan tersebut tentu akan mengganggu kinerja dari Sistem Event dalam memberikan layanan baik kepada *Organizer* maupun Member. Oleh karena itu, dalam penelitian ini akan menguji implementasi dari teknologi Blockchain dalam mengamankan proses pendaftaran event.

DOI: http://dx.doi.org/10.22441/fifo.2020.v12i1.007

II. Metodologi Penelitian

2.1. Studi Literatur

Tahap ini merupakan tahap melakukan pengumpulan data baik mengenai sistem yang akan digunakan untuk penelitian dan juga metode pengamanan yang akan diimplementasikan. Sehingga dapat diketahui gambaran akan kelebihan dan kekurangan ketika metode tersebut diimplementasikan.

Pengumpulan data dilakukan untuk memperoleh data yang dibutuhkan dalam pembuatan sebuah program aplikasi. Dalam penelitian ini teknik pengumpulan data dilakukan dengan beberapa metode sebagai berikut:

- Studi Pustaka

Metode ini dilakukan dengan membaca beberapa literatur baik berupa buku, jurnal penelitian terdahulu, makalah maupun artikel yang sesuai atau relevan dengan topik penelitian ini.

- Pengumpulan Data dari Internet

Metode ini dilakukan dengan cara mencari dan memilah informasi maupun data baik jurnal, website maupun prosiding yang memiliki kaitan dan dapat digunakan dalam penelitian ini.

2.2. Analisis

Tahap ini merupakan tahap untuk melakukan analisis kondisi saat ini mengenai subjek penelitian dan percobaan serangan sebelum diimplementasikan konsep pengamanan yang ditawarkan. Serangan yang diujicobakan berupa serangan DDoS pada Sistem Event. Hasil dari tahap ini akan diperoleh sebuah alur sistem dan kerentanan pada Sistem Event.

2.3. Desain

Pada tahap ini akan dipaparkan dan ditampilkan gambaran mengenai proses pendaftaran event. Gambaran dilakukan dengan menunjukkan diagram alir atau flowchart. Flowchart merupakan diagram yang digunakan untuk mewakili instruksi. Flowchart memiliki simbol standar untuk mewakili berbagai jenis instruksi. Simbol-simbol ini digunakan untuk membangun flowchart dengan proses step-by-step untuk masalah tersebut [15]. Flowchart yang telah dibuat akan dikonversikan menjadi diagram konseptual, sehingga proses terjadi dapat dipahami dengan lebih jelas.

2.4. Implementasi

Berdasarkan analisis yang dilakukan pada tahap sebelumya, akan memberikan gambaran mengenai kerentanan yang terdeteksi pada Sistem Event. Penelitian ini merupakan percobaan pengimplementasian dari teknologi Blockchain untuk mengamankan informasi pendaftaran event pada Sistem Event.

2.5. Pengujian

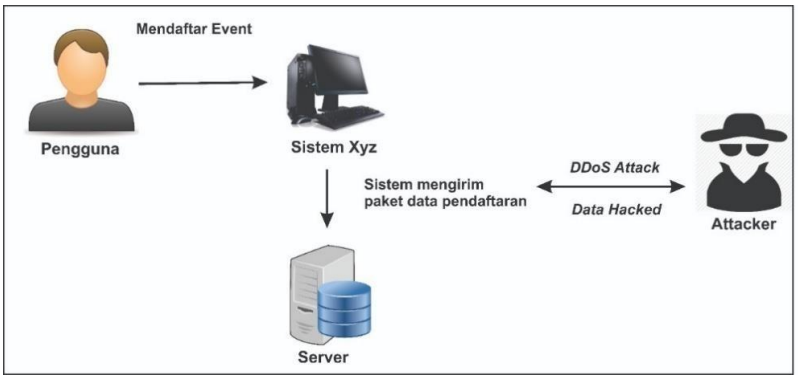
Implementasi yang telah dilakukan pada tahap sebelumnya akan diuji apakah *patch* yang dilakukan dapat mengamankan informasi pendaftaran event pada Sistem Event. Tahap ini merupakan tahap pengujian dari implementasi teknologi Blockchain yang dilakukan pada Sistem Event menggunakan *White Box Testing.*

III. Hasil dan Pembahasan

Gambar 1 memaparkan proses pendaftaran event seorang Member. Proses pendaftaran event dimulai dengan member melakukan registrasi sistem untuk mendapatkan *username* dan password, keamanan data dapat ditingkatkan dengan password dan pengaturan hak. Member yang telah memiliki *username* dan password melakukan *log-in* ke Sistem Event. Member yang berhasil melakukan *log-in* akan mendapatkan *privilege* untuk melakukan pendaftaran pada sebuah event yang ada pada Sistem Event.

Proses pendaftaran saat ini belum diimplementasikan keamanan sehingga informasi pendaftaran yang ter-*record* dan tersimpan dalam basisdata masih rentan akan serangan. Proses pendaftaran event juga belum ada proses validasi sebelum informasi yang dimasukkan ter-*record*, sehingga rentan akan duplikasi data, ketidakkonsistenan data, juga serangan DDoS.

Gambar 3 memaparkan desain konseptual kondisi saat ini dari Sistem Event. Member menginputkan data diri kedalam Sistem Event. Kemanan pada Sistem Event yang belum diimplementasikan keamanan dan validasi rentan akan serangan.



Gambar 3. Desain Konseptual Proses Pendaftaran Event Saat Ini

Pengimplementasian dari teknologi Blockchain pada Sistem Event dapat mengamankan informasi pendaftaran event. Blockchain memiliki tiga teknik/mekanisme antara lain adalah penggunaan *hash*, mekanisme *proof-of-work*, dan pengelolaan secara terdistribusi [13].

Mekanisme pertama adalah pemanfaatan teknik *hash*, dengan memanfaatkan teknik *hash* dari kriptografi, blok akan memiliki nilai *hash* yang mengidentifikasi blok dan seluruh isinya dan bersifat unik. Saat blok dibuat nilai *hash*-nya sekaligus dihitung. Mengubah sesuatu dalam blok akan mengakibatkan nilai *hash*-nya berubah. Dengan kata lain, nilai *hash* bermanfaat untuk mendeteksi perubahan blok. Elemen ketiga dari blok adalah nilai *hash* dari blok sebelumnya. Teknik memanfaatkan *hash* inilah yang membuat blockchain menjadi lebih aman, karena jika ada yang mengubah salah satu blok dalam rantai blok maka nilai *hash*-nya akan berubah dan blok berikutnya akan menjadi tidak valid lagi karena tidak menyimpan nilai *hash* yang valid dari blok sebelumnya.

Artinya, perubahan yang dilakukan terhadap sebuah blok akan mengakibatkan seluruh rantai blok menjadi tidak valid [13]. Contoh hasil dari pembuatan blok dapat dilihat pada Gambar 4.

Gambar 4. Hasil Pembuatan Rantai Blok

Mekanisme yang kedua adalah mekanisme *proof-of-work*. Mekanisme ini adalah mekanisme untuk memperlambat pembuatan blok baru. Mekanisme ini hadir dengan tujuan untuk mempersulit perubahan sebuah blok karena mengubah sebuah blok berarti harus menghitung *proof-of-work* seluruh blok. Dalam kasus bitcoin dibutuhkan waktu 10 menit untuk membuat blok baru dan menambahkan blok ke rantai [13]. Gambar 5 memaparkan contoh implementasi dari mekanisme *proof-of-work*, dimana setiap penambahan rantai blok akan mendapatkan *delay* waktu untuk menanggulagi serangan DDoS. Adapun perbandingan lama waktu pembuatan blok sebelum dan sesudah diimplementasikan mekanisme ini dapat dilihat pada Tabel 1.

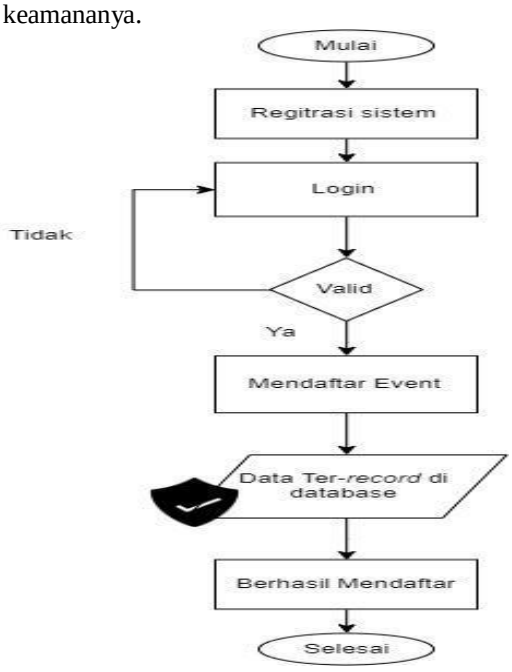
Gambar 5. Hasil Implementasi *Proof-of-work*

Tabel 1. Hasil Perbandingan Lama Pembuatan Blok Terhadap Implementasi *Proof-of-work*

Blok ke-	Sebelum (ms)	Sesudah (ms)
1	8.340400010347366	256.8270999789238
2	1.7521009743213654	830.44240000844
3	1.4425000250339508	360.1956999897957
4	1.6327989995479584	565.6066000163555

Proses pendaftaran event pada Gambar 6 menggambarkan alur proses pendaftaran event setelah diimplementasikan teknologi Blockchain, dimulai dengan member melakukan registrasi sistem untuk mendapatkan *username* dan password, keamanan data dapat ditingkatkan dengan password dan pengaturan hak. Member yang telah memiliki *username* dan password melakukan *log-in* ke Sistem Event. Member yang berhasil melakukan *log-in* akan mendapatkan *privilege* untuk melakukan pendaftaran pada sebuah event yang ada pada Sistem Event.

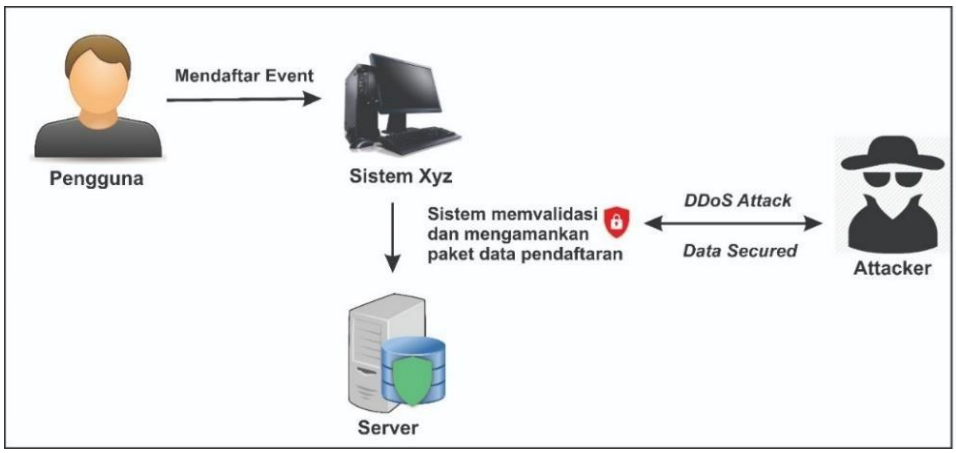
Proses pendaftaran event sebelum diimplementasikan keamanan, informasi dan proses pendaftaran yang ter-*record* dan tersimpan dalam basisdata masih rentan akan serangan. Setelah diimplementasikan teknologi Blockchain, informasi yang ter-*record* dan tersimpan dalam basisdata sebelumnya akan divalidasi dan dienkripsi terlebih dahulu, sehingga proses pendaftaran event yang telah diimplemantasikan teknologi Blockchain akan lebih terjamin keamananya.



Gambar 6. Flowchart Proses Pendaftaran Event Setelah Dilakukan Pengamanan

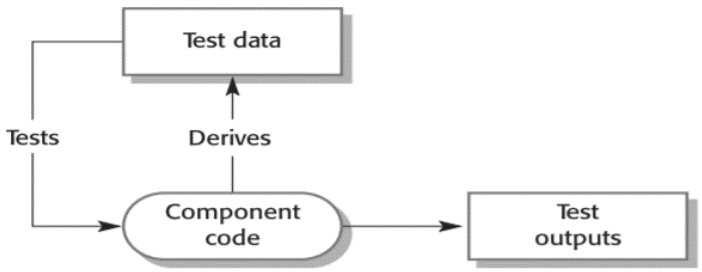
DOI: http://dx.doi.org/10.22441/fifo.2020.v12i1.007

Gambar 7 memaparkan desain konseptual dari alur proses pendaftaran event pada Sistem Event setelah diimplementasikan teknologi Blockchain. Data pengguna yang melakukan pendaftaran event pada Sistem Event akan divalidasi dan dienkripsi terlebih dahulu sebelum di-*record* di server, sehingga data akan lebih aman dari serangan.



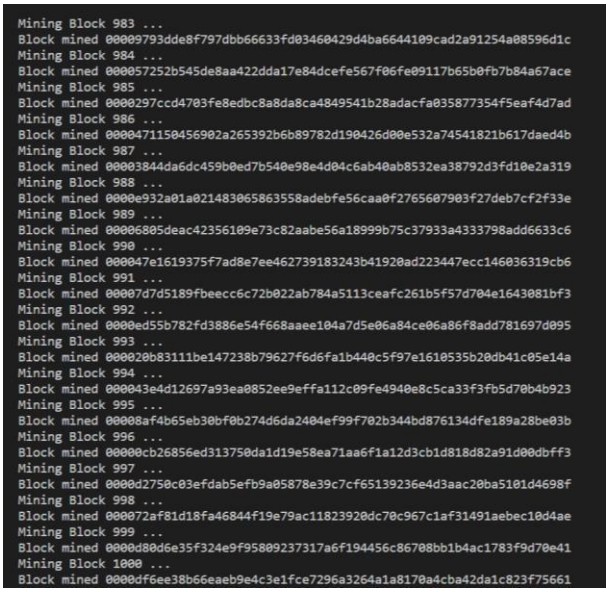
Gambar 7. Desain Konseptual Proses Pendaftaran Event Setelah Diimplementasikan Teknologi Blockchain

Metode pengujian yang dilakukan menggunakan metode *White Box Testing* seperti yang ditampilkan pada Gambar 8 [16], dimana pengembang melakukan uji keamanan dengan percobaan serangan terhadap sistem yang dikembangkan setelah patch diimplementasikan. *White Box Testing* adalah metode desain *test case* yang menggunakan struktur kendali dari pengembang [17]. *White Box Testing* dilakukan untuk mendeteksi kesalahan dan untuk mengetahui kompleksitas kode program [18]. *White Box Testing* sangat meningkatkan efektivitas *testing* secara keseluruhan, hal ini dapat lebih mudah mendeteksi *bug* yang sulit ditemukan dengan pengujian *Black Box Testing* atau metode pengujian lainnya, oleh karena itu Seorang *White Box Tester* harus memiliki pengetahuan mengenai struktur pemrograman [19], [20].



Gambar 8. White Box Testing

Hasil pengujian dari proses *White Box Testing* dapat dilihat pada Gambar 9. Simulasi serangan DDoS yang dilakukan pada pengujian ini adalah dengan membanjiri *request* paket pada sistem sebanyak 1000 paket dalam satu waktu.



Gambar 9. Hasil *White Box Testing*

IV. Kesimpulan dan Saran

4.1.Kesimpulan

Sistem Event memiliki celah kerentanan seperti akan serangan *Distributed Denial of Service* (DDoS) karena pada proses pendaftaran event belum diamankan dan divalidasi sebelum data-data tersebut di-*record* ke dalam basisdata. Teknologi Blockchain memiliki dua teknik/mekanisme antara lain adalah penggunaan *hash* dan mekanisme *proof-of-work* yang dapat menjadi alternatif pengamanan informasi pemdaftaran event karena dapat menjaga keamanan informasi, kekonsistenan data, dan serangan dari DDoS.

4.2. Saran

Saran untuk penelitian selanjutnya dapat dilakukan analisis perbandingan dari metode-metode penanggulangan serangan DDoS yang sudah ada dengan mekanisme-mekanisme yang ada pada teknologi Blokchain, sehingga dapat diketahui metode yang lebih baik untuk menanggulangi serangan DDoS.

V. Daftar Pustaka

[1] Riadi, I., Sunardi., & Muhammad, A. W. 2018. DDoS Detection Using Artificial Neural Network Regarding Variation of Training Function. *Advanced Science Letters*. Vol. 24(12), pp. 9163-9167.

[2] Yudhana, A., Riadi, I., & Ridho, F. 2018. DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics. *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 9(11), pp. 177-183.

[3] Fadlil, A., Riadi, I., & Aji, S. 2017. DDoS Attacks Classification using Numeric Attribute-based Gaussian Naive Bayes. *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 8(8), pp. 42-50.

[4] Aziz, M., Umar, R., Ridho, F. 2019. Implemetasi Jaringan Saraf Tiruan Untuk Mendeteksi Serangan DDoS Pada Forensik Jaringan. *Query: Journal of Information Systems.* Vol. 3(1), pp. 46-52.

[5] Muhammad, A. W., Riadi, I., & Sunardi. 2017. Deteksi Serangan DDoS Menggunakan Neural Network dengan Fungsi Fixed Moving Average Window. *JISKa*, Vol. 1(3), pp. 115-122.

[6] Hermawan, R. (2012). Analisis konsep dan cara kerja serangan komputer *distributed denial of service* (DDoS). *Faktor Exacta*, vol. 5(1), 1-14.

[7] Kristanto, A. 2003. *Keamanan data pada jaringan komputer.* Yogyakarta: Gava Media.

[8] Kurniawan, Y. 2004. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung:

INFORMATIKA.

[9] S, L. Dito H., Toban, S. T. P., & Putra, P. W. 2019. *Mengenal DDoS attack dan solusinya*. Diambil pada tanggal 29 Oktober 2019, dari https://socs.binus.ac.id/2019/07/30/mengenal-ddos-attack-dan-solusinya-2/

[10] Putra, G. D., Sumaryono, S., Widyawan. Rancang Bangun Identity and Access Management IoT Berbasis KSI dan Permissioned Blockchain. *JNTETI*. Vol. 7(4), pp. 384-390.

[11] Harris, C. 21 Februari 2018. *The History of Bitcoin*. Diambil pada tanggal 29 Oktober 2019, dari https://cryptocurrencynews.com/the-history-of-bitcoin/

[12] Efanov, D. & Roschin, P. 2018. *The All-Pervasiveness of the Blockchain Technolo*gy. procediaComputer Science. pp. 116-121. Russia: Moscow.

[13] Noorsanti, R. C., Yulianton, H., & Hadiono, K. 2018. *Blockchain - Teknologi Mata Uang Kripto (Crypto Currency)*. Prosiding SENDI_U 2018. pp. 306-311. Semarang: Universitas Stikubank Semarang.

[14] Perdani, M. D. K., Widyawan., & Santosa, P. I. 2018. *Blockchain untuk keamanan transaksi elektronik perusahaan financial technology (studi kasus pada PT Xyz).* Seminar Nasional Teknologi Informasi dan Multimedia 2018. Vol. 6(1), pp. 7-12.

[15] KS3. 2019. *Designing an algorithm*. Diambil pada tanggal 5 Desember 2019, dari https://www.bbc.co.uk/bitesize/guides/z3bq7ty/revision/3

[16] Sommerville, I. 2011. *Software Engineering Ninth Edition*. Pearson Education, Inc. United States of America.

[17] Irawan, Y. 2017. Pengujian Sistem Informasi Pengelolaan Pelatihan Kerja UPT BLK Kabupaten Kudus dengan Metode *Whitebox Testing*. *Journal Speed – Sentra Penelitian Engineering dan Edukasi*. Vol. 9(3), pp. 59-63.

[18] Fakhri, M. A., Aknuranda, I., Pramono, D. 2018. Implementasi Sistem Informasi Showroom Mobil (SISMOB) dengan Pemrograman Berbasis Objek (Studi Kasus: UD. Tomaru Oto). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*. Vol. 2(9), pp. 2967-2974.

[19] Alfisahrin, S. N. N. 2012. Pendekatan *White Box Testing* Untuk Menentukan Kualitas Perangkat Lunak dengan Menggunakan Bahasa Pemrograman C++. *PARADIGMA*. Vol. 14(1), pp. 69-78.

[20] Alfaris, H. B. I., Anam, C., Masy'an, A. 2013. Implementasi Black Box Testing pada Sistem Informasi Pendaftaran Santri Berbasis Web Dengan Menggunakan PHP dan MySql. *SAINTEKBU: Jurnal Sains dan Teknologi*. Vol. 6(1), pp. 23-38