PERGURUAN TINGGI MUHAMMADIYAH
UNIVERSITAS AHMAD DAHLAN
LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
Jalan Gondosuli 1B Semaki, Yogyakarta 55166 Telp. (0274) 542886, Fax. (0274) 542886

SURAT PERJANJIAN PELAKSANAAN PENELITIAN

Nomor: PUPS-013/SP3/LPPM-UAD/2020

Pada hari ini, **Sabtu** tanggal **Delapan belas** bulan **April** tahun **Dua ribu dua puluh (18-04-2020)**, kami yang bertandatangan di bawah ini:

1. Nama : **Dr. Widodo, M.Si.**
   Jabatan : Kepala Lembaga Penelitian dan Pengabdian Kepada Masyarakat Universitas Ahmad Dahlan (LPPM UAD), selanjutnya disebut sebagai **PIHAK PERTAMA.**
2. Nama : **IMAM RIADI. Dr.. M.Kom**
   Jabatan : Dosen/Peneliti pada Program Studi **Sistem Informasi Fakultas Sain dan Teknologi Terapan (FAST)** Universitas Ahmad Dahlan (UAD), selaku Ketua Peneliti, selanjutnya disebut **PIHAK KEDUA.**

Kedua belah pihak menyatakan setuju dan mufakat untuk mengadakan perjanjian pelaksanaan penelitian untuk selanjutnya disebut Surat Perjanjian Pelaksanaan Penelitian (SP3) dengan ketentuan dan syarat-syarat sebagai berikut.

Pasal 1

DASAR HUKUM

(1) Hasil *review*/penilaian proposal yang dilakukan oleh Tim Reviewer Penelitian Internal UAD.
(2) Surat Keptusan Kepala LPPM UAD nomor: L1/098/I.0/IV/2020 tanggal 15 April 2020 tentang Penetapan Hasil Seleksi Proposal Penelitian Dana UAD Tahun Akademik 2019/2020.

Pasal 2

RUANG LINGKUP

(1) PIHAK PERTAMA memberikan pekerjaan kepada PIHAK KEDUA dan PIHAK KEDUA menyatakan menerima pekerjaan dari PIHAK PERTAMA berupa kegiatan penelitian sebagai berikut.

Skema	:	Penelitian Unggulan Program Studi (PUPS)
Judul penelitian	:	Optimasi Keamanan IoT Terhadap Serangan Cross Site Scripting (XSS) Menggunakan Teknologi Blockchain
Jenis Riset	:	Riset Terapan (RT) , TKT: 5
Mitra Penelitian	:	ATTCDV (Amnotel Cyber Digital Valley)
Luaran Wajib	:	Artikel pada Jurnal

(2) Jangka waktu penelitian tersebut pada ayat (1) paling lama **6 (enam) bulan** sejak ditandatangani SP3 ini, dan menyerahkan hasil laporan penelitian sementara kepada PIHAK PERTAMA selambat-lambatnya pada **18 Oktober 2020.**
(3) PIHAK KEDUA berkewajiban untuk merealisasikan luaran penelitian seperti yang dijanjikan dalam proposal penelitian.

Pasal 3

PERSONALIA PELAKSANA PENELITIAN

Personalia pelaksana penelitian ini terdiri dari:

Ketua Peneliti	: IMAM RIADI. Dr.. M.Kom
Pembimbing	
Anggota 1	: RUSYDI UMAR. S.T.. M.T.. P.hD.
Anggota 2	: -

Paraf: .....

Pasal 4

BIAYA PENELITIAN DAN CARA PEMBAYARAN

(1) PIHAK PERTAMA menyediakan dana pelaksanaan penelitian kepada PIHAK KEDUA sejumlah **Rp 20,000,000,00 (Duabelas Juta rupiah)** yang dibebankan pada Anggaran Pendapatan dan Belanja (APB) LPPM UAD Tahun Akademik 2019/2020 dibayarkan melalui rekening bank atas nama Ketua Peneliti oleh Bidang Finansial UAD sebagai berikut.

Nama : IMAM RIADI. Dr.. M.Kom
Nama Bank : BPD DIY SYARIAH
Nomor rekening : 801,211,007,878

(2) **Tahap I sebesar 60% x Rp 20,000,000,00 = Rp 12,000,000,00** (Duabelas Juta rupiah), dibayarkan setelah SP3 ini ditandatangani oleh PARA PIHAK dan PIHAK KEDUA telah mengunggah file scan SP3 ini pada portal UAD selambat-lambatnya pada Juni 2020.

(3) **Tahap II sebesar 40% x Rp 20,000,000,00 = Rp 8,000,000,00** (Delapan Juta rupiah), dibayarkan setelah: (a) PIHAK KEDUA mengunggah revisi laporan akhir pasca kolokium dan (b) luaran wajib penelitian telah submit (minimal) untuk jenis luaran jurnal/seminar, atau tersedia draft untuk jenis luaran buku/naskah akademik, atau telah mendaftarkan kekayaan intelektual (KI) untuk jenis luaran paten dan hak cipta dan jenis KI lainnya, dan sejenisnya.

Jika PIHAK KEDUA hanya melakukan poin (a) sedangkan poin (b) TIDAK TERPENUHI, maka dana penelitian tahap II hanya dapat dicairkan sebesar 20%.

Pasal 5

PELAKSANAAN PEMBIMBINGAN

(1) Khusus skema Penelitian Dosen Pemula (PDP), peneliti wajib melakukan pembimbingan atau konsultasi dengan dosen pembimbing penelitiannya paling sedikit 4 (empat) kali pembimbingan.

(2) Pembimbingan sebagaimana dimaksud dalam ayat (1) minimal dalam hal-hal sebagai berikut.
a. penyusunan angket/kuesioner dan atau teknik pengumpulan data lainnya;
b. analisis data dan interpretasinya;
c. penyusunan hasil penelitian, pembahasan, penarikan kesimpulan;
d. penyusunan kuaran penelitian.

(3) Pembimbingan sebagaimana dimaksud dalam ayat (1) dan ayat (2) dituliskan dalam form pembimbingan yang ditandatangani oleh peneliti dan dosen pembimbing penelitian.

Pasal 6

JENIS LAPORAN PENELITIAN

(1) PIHAK KEDUA wajib menyusun dan menyampaikan laporan penelitian baik secara *on line* melalui portal UAD maupun *hardcopy* kepada PIHAK PERTAMA yang terdiri atas:
a. Laporan Kemajuan
b. Laporan Sementara
b. Laporan Akhir Penelitian

(2) Berkas **Laporan Kemajuan** digunakan sebagai bahan monitoring dan evaluasi (monev) internal.

(3) Berkas **Laporan Sementara** digunakan sebagai bahan kolokium laporan penelitian.

(4) Berkas **Laporan Akhir Penelitian** merupakan revisi dari Laporan Penelitian Sementara pasca kolokium.

Paraf: .....

Pasal 7

MONITORING DAN EVALUASI

(1) PIHAK PERTAMA berhak untuk melakukan monitoring dan evaluasi (monev) internal pelaksanaan penelitian, baik secara administrasi maupun substansi.

(2) Pemantauan kemajuan penelitian dilakukan oleh Tim Monev yang dibentuk oleh PIHAK PERTAMA.

(3) PIHAK KEDUA diharuskan MENYIAPKAN SEMUA DOKUMEN/BUKTI kemajuan pelaksanaan penelitiannya guna kepentingan monev.

(4) Waktu pelaksanaan monev akan ditentukan oleh PIHAK PERTAMA.

Pasal 8

KOLOKIUM LAPORAN PENELITIAN

(1) PIHAK KEDUA wajib menyerahkan **Laporan Penelitian Sementara** sebagai bahan kolokium selambat-lambatnya **18 Oktober 2020.**

(2) Ketua Peneliti wajib hadir dan mempresentasikan hasil penelitiannya pada kolokium **Laporan Penelitian Sementara** yang pelaksanaannya akan diatur oleh PIHAK PERTAMA.

(3) Revisi laporan penelitian yang sudah dikolokiumkan harus mendapatkan pengesahan dari *reviewer* dalam bentuk **Surat Pernyataan** dan dijilid dalam satu kesatuan laporan penelitian.

Pasal 9

LAPORAN AKHIR PENELITIAN

(1) PIHAK KEDUA wajib menyerahkan **Laporan Akhir Penelitian** selambat-lambatnya **2 (dua) pekan** setelah dikolokiumkan.

(2) Penyusunan laporan penelitian mengacu pada ketentuan dalam Pedoman Penelitian yang dikeluarkan oleh LPPM dan ketentuan lain yang berlaku.

(3) Laporan Akhir Penelitian sebagaimana tersebut pada ayat (1) dan (2) harus memenuhi ketentuan sebagai berikut:
a. bentuk/ukuran kertas A4;
b. warna cover sesuai ketentuan;
c. di bawah bagian cover ditulis:

PENELITIAN INI DILAKSANAKAN ATAS BIAYA
ANGGARAN PENDAPATAN DAN BELANJA UNIVERSITAS AHMAD DAHLAN
TAHUN AKADEMIK 2019/2020
NOMOR KONTRAK: PUPS-013/SP3/LPPM-UAD/2020

(4) PIHAK KEDUA wajib mengunggah file laporan akhir penelitian secara lengkap pada alamat http://www.simpel.uad.ac.id melalui akun portal ketua peneliti dengan format file PDF.

Pasal 10

TANGGUNGAN PENELITIAN DAN LUARAN PENELITIAN

(1) Peneliti dinyatakan memiliki **tanggungan atau hutang penelitian** apabila sampai pada masa penerimaan proposal penelitian periode berikutnya belum menyelesaikan kewajibannya.

(2) Peneliti yang memiliki tanggungan penelitian sebagaimana dimaksud pada ayat (1) tidak diperkenankan mengajukan proposal penelitian pada periode tersebut.

(3) Peneliti dinyatakan memiliki **tanggungan atau hutang luaran penelitian** apabila sampai pada masa pengumpulan revisi laporan akhir penelitian pasca kolokium target luaran wajib penelitiannya belum submit (minimal) untuk jurnal/seminar, atau tersedia draft buku/naskah akademik, atau mendaftarkan kekayaan intelektual (KI), dan sejenisnya.

Paraf: .....

(4) Peneliti yang memiliki tanggungan luaran penelitian sebagaimana dimaksud pada ayat (3) masih diperkenankan mengajukan proposal penelitian pada periode tersebut.

(5) Peneliti yang belum memenuhi luaran wajib berupa *accepted* (minimal) untuk jurnal/seminar, atau terbit buku/naskah akademik, atau tersedia sertifikat kekayaan intelektual (KI), dan sejenisnya selama dua periode penelitian berturut, tidak diperkenankan mengajukan proposal penelitian pada periode tersebut.

Pasal 11

SANKSI DAN PEMUTUSAN PERJANJIAN PENELITIAN

(1) PIHAK PERTAMA berhak memberikan peringatan dan atau teguran atas kelalaian dan atau pelanggaran yang dilakukan oleh PIHAK KEDUA yang mengakibatkan tidak dapat terpenuhinya kontrak penelitian ini.

(2) PIHAK PERTAMA berhak melakukan pemutusan perjanjian penelitian, jika PIHAK KEDUA tidak mengindahkan peringatan yang diberikan oleh PIHAK PERTAMA.

(3) Segala kerugian material maupun finansial yang disebabkan akibat kelalaian PIHAK KEDUA, maka sepenuhnya menjadi tanggungjawab PIHAK KEDUA.

(4) Jenis sanksi yang diberikan dapat berupa:
   (a) tidak diperkenankannya mengajukan proposal penelitian sebagaimana dimaksud pada Pasal 10 ayat (5) sampai kewajibannya terselesaikan; dan atau
   (b) tidak dapat mencairkan dana tahap 2; dan atau
   (c) mengembalikan dana yang telah diterima oleh PIHAK KEDUA.

Pasal 12

KEADAAN MEMAKSA (*FORCE MAJEUR*)

Ketentuan dalam Pasal 10 tersebut di atas tidak berlaku dalam keadaan sebagai berikut:

a. Keadaan Memaksa (*force majeur*)

b. PIHAK PERTAMA menyetujui atas terjadinya keterlambatan yang didasarkan pada pemberitahuan sebelumnya oleh PIHAK KEDUA kepada PIHAK PERTAMA dengan **surat pemberitahuan** mengenai kemungkinan terjadinya keterlambatan dalam penyelesaian kegiatan penelitian sebagaimana dimaksud dalam Pasal 1 dan Pasal 3; dan sebaliknya PIHAK KEDUA menyetujui terjadinya keterlambatan pembayaran sebagai akibat keterlambatan dalam penyelesaian perjanjian penelitian.

Pasal 13

(1) Keadaan Memaksa (*force majeur*) sebagaimana yang dimaksud dalam Pasal 12 ayat (1) adalah peristiwa-peristiwa yang secara langsung mempengaruhi pelaksanaan perjanjian serta terjadi di luar kekuasaan dan kemampuan PIHAK KEDUA ataupun PIHAK PERTAMA.

(2) Peristiwa yang tergolong dalam keadaan memaksa (*force majeur*) antara lain berupa bencana alam, pemogokan, wabah penyakit, huru-hara, pemberontakan, perang, waktu kerja diperpendek oleh pemerintah, kebakaran dan atau peraturan pemerintah mengenai keadaan bahaya serta hal-hal lainnya yang dipersamakan dengan itu, sehingga PIHAK KEDUA ataupun PIHAK PERTAMA terpaksa tidak dapat memenuhi kewajibannya.

(3) Peristiwa sebagaimana dimaksud pada ayat (2) tersebut di atas, wajib dibenarkan oleh penguasa setempat dan diberitahukan dengan Surat oleh PIHAK KEDUA atau PIHAK PERTAMA kepada PIHAK PERTAMA atau PIHAK KEDUA selambat-lambatnya 7 (tujuh) hari sejak terjadinya peristiwa yang dikategorikan sebagai Keadaan Memaksa (*force majeur*).

(4) PIHAK PERTAMA memberikan kesempatan kepada PIHAK KEDUA untuk menyelesaikan perjanjian kontrak ini sampai pada batas waktu yang disepakati oleh kedua belah pihak jika keadaan *force majeur* dinyatakan telah selesai.

Paraf: .....

Pasal 14

PENYELESAIAN PERSELISIHAN

(1) Apabila dalam pelaksanaan perjanjian dan segala akibatnya timbul perbedaan pendapat atau perselisihan, PIHAK PERTAMA dan PIHAK KEDUA setuju untuk menyelesaikannya secara musyawarah untuk mencapai mufakat.

(2) Apabila penyelesaian sebagaimana termaksud dalam ayat (1) di atas tidak tercapai, maka PIHAK PERTAMA dan PIHAK KEDUA sepakat menyerahkan perselisihan tersebut melalui mediasi dengan Rektor sebagai atasan langsung dari PIHAK PERTAMA yang putusannya bersifat final dan mengikat.

Pasal 15

PENGUNDURAN DIRI

(1) Apabila PIHAK KEDUA mengundurkan diri atau membatalkan SP3 ini, maka PIHAK KEDUA wajib mengajukan Surat Pengunduran Diri yang ditujukan kepada PIHAK PERTAMA.

(2) Surat Pengunduran Diri sebagaimana dimaksud pada ayat (1) wajib disahkan oleh Dekan fakultas ketua peneliti yang bersangkutan; dan bagi peneliti skim PDP ditambah persetujuan Dosen Pembimbing.

(3) PIHAK KEDUA wajib mengembalikan dana yang telah diterima kepada PIHAK PERTAMA

Pasal 16

LAIN-LAIN

(1) Hal-hal yang dianggap belum cukup dan perubahan-perubahan perjanjian akan diatur kemudian atas dasar permufakatan kedua belah pihak yang akan dituangkan dalam bentuk Surat atau Perjanjian Tambahan (*addendum*), yang merupakan kesatuan dan bagian yang tidak terpisahkan dari perjanjian awal.

(2) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini berlaku sejak ditandatangani dan disetujui oleh kedua belah pihak.

PIHAK PERTAMA,

Dr. Widodo, M.Si.
NIP: 19600221198709101

PIHAK KE DUA,

METERAI TEMPEL
8000D8AHF458692159
6000
ENAM RIBU RUPIAH

IMAM RIADI. Dr.. M.Kom
NIP/NIY. 60020397

Paraf: .....

Kode/Nama Rumpun Ilmu: 458 / Teknik Informatika

LAPORAN AKHIR

PENELITIAN UNGGULAN PROGRAM STUDI

OPTIMASI KEAMANAN IOT TERHADAP SERANGAN *CROSS-SITE SCRIPTING* (XSS) MENGGUNAKAN TEKNOLOGI BLOCKCHAIN

Disusun Oleh:

Dr. Imam Riadi/0510088001

Rusydi Umar/0507087202

MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS AHMAD DAHLAN

JANUARI 2021

HALAMAN PENGESAHAN

LAPORAN PENELITIAN UNGGULAN PROGRAM STUDI
TAHUN AKADEMIK 2019 / 2020

Judul Penelitian	: Optimasi Keamanan IoT Terhadap Serangan *Cross-Site Scripting* (XSS) Menggunakan Teknologi Blockchain.
Kode/Nama Rumpun Ilmu	: 458 / Teknik Informatika
Butir RIP	: Topik 5 : Teknologi Informasi dan Komunikasi
TSE Penelitian	: Information, computer and communication

Ketua Peneliti

a. Nama Lengkap	: Dr. Imam Riadi, M.Kom
b. NIY	: 60020397
c. Jabatan Fungsional	: Lektor Kepala
d. Program Studi	: Sistem Informasi
e. Nomor HP	: 08156854308
f. Alamat surel (e-mail)	: imam.riadi@is.uad.ac.id

Anggota Peneliti (1)

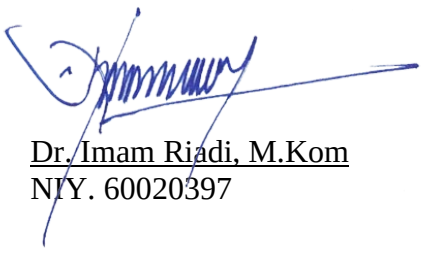
a. Nama Lengkap	: Rusydi Umar, S.T., M.T., Ph.D
b. NIY	: 60980174
c. Perguruan Tinggi	: Universitas Ahmad Dahlan

Lokasi Penelitian	: Yogyakarta
Lama Penelitian Keseluruhan	: 6 bulan
Biaya Penelitian Keseluruhan	: Rp. 20.000.000,-
Tahun 1	: Rp. 20.000.000,-
Tahun 2	: -

Mengetahui,
Dekan Fakultas Teknologi Industri

Sunardi., S.T., M.T., Ph.D
NIY. 60010313

Yogyakarta, 25 Januari 2021
Ketua Peneliti,



Dr. Imam Riadi, M.Kom
NIY. 60020397

Menyetujui,
Kepala Lembaga Penelitian dan Pengabdian kepada Masyarakat
Universitas Ahmad Dahlan,

Anton Yudhana, S.T., M.T., Ph.D.
NIY. 60010383

DAFTAR ISI

Halaman Pengesahan i
Surat Pernyataan Telah Revisi..... ii
Daftar Isi..... iii
Daftar Tabel..... iv
Daftar Gambar v
Abstrak vi
Abstract vii
Prakata..... viii
Laporan Akhir Penelitian 1
I. Identitas Penelitian..... 1
II. Substansi Penelitian..... 2
Lampiran 15

DAFTAR TABEL

Tabel 1. Alat Penelitian..... 4
Table 2. Setting Cable RS232 to NodeMCU 5

DAFTAR GAMBAR

Gambar 1. Perancangan IoT Transaksi Pembayaran 5
Gambar 2. Perancangan IoT Transaksi Pembayaran 6
Gambar 3. Hasil Pengujian Kerentanan 7
Gambar 4. Implementasi Blockchain 8
Gambar 5. Hasil Pengujian Kerentanan setelah Implementasi Blockchain 10

ABSTRAK

Era digital merupakan zaman dimana semua orang sudah menggunakan teknologi dan mereka saling terkoneksi satu sama lain dengan sangat mudah. Salah satu teknologi yang muncul diera revolusi industri 4.0 adalah internet of thing (IoT). IoT pada penelitian ini digunakan sebagai media pengiriman data transaksi pembayaran agar dapat tersimpan di server REST API, dirancang menggunakan RS232 dan NodeMCU. Data transaksi yang dikirimkan menggunakan IoT ini sangat rentan dari berbagai jenis serangan jika tidak diamankan, salah satunya rentan dari serangan cross-site scripting (XSS). Peretas dapat mencuri, mengubah, bahkan menghapus data transaksi pembayaran yang sudah dikirimkan IoT di REST API, sehingga keamanan nya sangat perlu ditingkatkan agar data yang tersimpan aman dari serengan peretas.

Optimasi keamanan pada penelitian ini dilakukan dengan implementasi blockchain. Blockchain yang memiliki keunggulan dari sisi keamanan ini diharapkan dapat mengamankan data transaksi pembayaran yang tersimpan di REST API. Penelitian ini dilakukan dengan beberapa tahap, pertama pengumpulan peralatan penelitian, kedua perencangan IoT, ketiga pengujian kerentanan, keempat implementasi blockchain dan terakhir pengujian kerentanan setelah implementasi blockchain.

Hasil yang diperoleh dari penelitian ini yaitu implementasi blockchain untuk meningkatkan keamanan pada IoT transaksi pembayaran agar terhindar dari serangan XSS berhasil dilakukan. Dibuktikan dengan hasil pengujian kerentanan IoT transaksi pembayaran sebelum dan sesudah implementasi blockchain, sebelum implementasi blockchain dilakukan hasil pengujian kerentanan IoT transaksi pembayaran dinyatakan bahwa ditemukan 1 celah kerentanan XSS yang memiliki tingkat risiko keseluruhan berlevel tinggi, sedangkan hasil dari pengujian kerentanan setelah implementasi blockchain dilakukan adalah tidak ditemukannya kerentanan dari serangan XSS (celah kerentanan XSS nya 0 atau tidak ditemukan).

Kata kunci: Blockchain, Internet of Things, XSS Attack, Security

ABSTRACT

One of the technologies that emerged in the era of the 4.0 industrial revolution is the internet of things (IoT). IoT in this study is used as a medium for sending payment transaction data so that it can be stored on the REST API server. Transaction data sent using IoT is very vulnerable to various types of attacks if it is not secured, one of which is vulnerable to cross-site scripting (XSS) attacks. Hackers can steal, change, and even delete payment transaction data that IoT has sent in the REST API so that security needs to be improved. Security optimization in this study was carried out by implementing blockchain. Blockchain, which has the advantage the security, is expected to be able to secure payment transaction data stored in the REST API.

This research was carried out in several stages, first the collection of research tools, second IoT planning, third vulnerability testing, fourth blockchain implementation and, finally vulnerability testing after blockchain implementation.

The results obtained from this study are the implementation of blockchain to increase security on IoT payment transactions to avoid successful XSS attacks. Evidenced by the results of payment transaction IoT vulnerability testing before and after blockchain implementation, prior to blockchain implementation, the payment transaction IoT vulnerability testing results stated that 1 XSS vulnerability was found which had a high level of overall risk, while the results of vulnerability testing after blockchain implementation were not found a vulnerability from an XSS attack (its XSS vulnerability gap was 0 or not found).

Keywords: Blockchain, Internet of Things, XSS Attack, Security

PRAKATA

Alhamdulillah Kami ucapkan puji syukur kehadirat Allah SWT sehingga terselesaikannya Penelitian Unggulan Program Studi (PUPS) dengan dana Universitas Ahmad Dahlan tahun anggaran 2021. Dalam penelitian ini, Kami melibatkan 5 orang staf pendukung dan dua orang dosen yang berjudul Optimasi Keamanan IoT Terhadap Serangan *Cross-Site Scripting* (XSS) Menggunakan Teknologi Blockchain.

Laporan penelitian ini telah mencapai tahap penyelesaian dan mendapatkan hasil seperti yang diinginkan. Sampai akhir dari waktu penelitian ini, yakni selama 10 bulan, penelitian yang dilakukan memberikan hasil 100%.

Terimakasih atas Kami sampaikan kepada LPP-UAD yang telah mengamanahi kami dengan memberikan hibah untuk penelitian kerjasama Kelembagaan. Terima kasih juga kepada Universitas Ahmad Dahlan dalam hal ini adalah LPP UAD sebagai wadah peneliti UAD. Terimakasih juga kami sampaikan kepada pihak-pihak terkait aras semua nasehat, masukan, dan kerjasama yang baik dalam upaya penyelesaian laporan penelitian ini.

Wassalammu'alaikum Wr. Wb.

Yogyakarta, 25 Januari 2021
Tim Peneliti

Imam Riadi/0510088001
Rusydi Umar/0507087202

LAPORAN AKHIR PENELITIAN

I. IDENTITAS PENELITIAN

A. JUDUL PENELITIAN

Judul	:	Optimasi Keamanan IoT terhadap Serangan *Cross Site Scripting* (XSS) Menggunakan Teknologi *Blockchain*
Skema	:	Prototipe
Jenis Riset	:	PUPS TKT: 3
Ketua peneliti	:	Dr. Imam Riadi, M.Kom
Anggota 1	:	Rusydi Umar, S.T., M.T., Ph.D
Anggota 2	:	Tri Lestari
Anggota 3		Iqbal Busthomi
Anggota 4		Achmad Nugrahantoro
Anggota 5		M. Nasir Hafizh
Anggota 6		Purwono
Pembimbing	:	

B. PRODUK/INOVASI PENELITIAN

No	Nama Produk/Inovasi Penelitian	Status	Keterangan
1	Sistem Top-Up Uang Saku	Prototipe	Dalam proses pengembangan

II. SUBSTANSI PENELITIAN

A.	**RINGKASAN:** Ringkasan penelitian berisi: (i) latar belakang penelitian, (ii) tujuan dan tahapan metode penelitian, (iii) luaran yang ditargetkan, serta (iv) uraian TKT penelitian yang diusulkan.

1.1 Latar Belakang

Perkembangan teknologi informasi serta jaringan internet yang semakin luas secara tidak langsung memberikan dampak pada pertumbuhan pengguna *smartphone*, penggunaan *smartphone* dimasa sekarang tidak hanya sekedar untuk melakukan panggilan telepon atau berkirim pesan singkat, tetapi penggunaan *smartphone* menjadi selayaknya komputer pribadi bagi penggunanya. Pada januari 2018 berdasarkan *system* operasi pengguna *smartphone* yang mengakses internet dengan perangkat *mobile* berbasis Android adalah sebanyak 73.5%, Apple IOS sebanyak 19.9%, dan *platform* lainnya sebanyak 6.6% (Kemp, 2018).

Manusia pada dasarnya merupakan makluk sosial, pada era teknologi sekarang media sosial menjadi salah satu alat untuk berinteraksi dengan manusia lainnya, selain untuk mengirim dan menerima informasi juga sebagai tempat untuk menyimpan suatu data infromasi dari pemilik akun media sosial. Berdasarkan pengguna aktif bulanan dari berbagai negara sebanyak 2.9 milyar pengguna media sosial menggunakan perangkat *mobile* dengan pengguna terbanyak dari Asia Timur sebanyak 64% (Kemp, 2018). Pada 2016 media sosial dengan pengguna paling banyak adalah Facebook 1.65 milyar, Instagram 500 juta pengguna dan Twitter 310 juta pengguna. Kejahatan pada media sosial Facebook dan Twitter meningkat sebanyak 780% selama 4 tahun dari tahun 2008 (556 kasus) sampai tahun 2012 (4908) kasus (Mukti, dkk, 2017).

Kemunculan suatu teknologi baru biasanya diiringi dengan munculnya suatu ancaman tindak kejahatan baru pula, perkembangan *smartphone* dan media sosial saat ini banyak disalahgunakan untuk melakukan tindak kejahatan (*cybercrime*) seperti *cyberbully*, penipuan, pemerasan, penyebaran *hoax*, ujaran kebencian dan lainnya. Pelaku kejahatan *cybercrime* biasanya dapat menghilangkan barang bukti

kejahatan dengan cara menghapus data sehingga secara langsung data tersebut tidak dapat terlihat lagi, oleh karena itu perlu adanya proses forensik terhadap perangkat *mobile* yang menggunakan media sosial untuk tindak kejahatan, dengan menggunakan *framework Digital Forensic Research Workshop* (DFRWS) untuk mendapatkan bukti digital tindak kejahatan dan diharapkan dapat menjadi bukti digital tindak kejahatan di media sosial.

1.2 Tujuan dan Tahapan Metode

Internet of Thing (IoT) yang dirancang harus dilengkapi dengan keamanan agar terhindar dari berbagai jenis serangan seperti cross site scripting (XSS), SQL injection, maupun serangan berbahaya lainnya. Penelitian ini dilakukan optimasi keamanan IoT transaksi pembayaran agar terhindar dari serangan khususnya cross site scripting (XSS). Serangan XSS dapat mengakibatkan keamanan pada sisi client ter-bypass sehingga penyerang dapat mencuri informasi sensitif dari pengguna, mengendalikan sesi, menjalankan kode jahat, dan menyimpan aplikasi berbahaya. Penelitian ini dilakukan dengan beberapa tahap. Pertama pengumpulan peralatan penelitian, kedua perancangan IoT, setelah itu diuji kerentanan, dilanjutkan dengan implementasi Blockchain dan dilakukan dengan pengujian kerentanan setelah implementasi Blockchain, diakhiri dengan penarikan hasil dan kesimpulan.

1.3 Luaran yang ditargetkan

Artikel ilmiah hasil pengimplementasian teknologi Blockchain pada sistem yang diuji dengan serangan-serangan siber, diantaranya serangan *cross site scripting* (XSS).

1.4 Uraian Hasil Penelitian

Hasil yang diperoleh dari penelitian ini sebelum implementasi Blockchain dilakukan tingkat risiko secara keseluruhan adalah ditemukan 1 celah kerentanan XSS yang memiliki tingkat risiko keseluruhan berlevel tinggi, kemudian hasil dari pengujian kerentanan setelah implementasi Blockchain dilakukan adalah tidak ditemukannya kerentanan dari serangan XSS.

B. KATA KUNCI: *Blockchain, Internet of Things, XSS Attack, Security*

C. HASIL PELAKSANAAN PENELITIAN: Tuliskan secara ringkas hasil pelaksanaan penelitian yang telah dicapai sesuai tahun pelaksanaan penelitian. Penyajian meliputi **data, hasil analisis, pembahasan hasil dan capaian luaran** (wajib dan atau tambahan). Seluruh hasil atau capaian yang dilaporkan harus berkaitan dengan tahapan pelaksanaan penelitian sebagaimana direncanakan pada proposal. Penyajian data dapat berupa gambar, tabel, grafik, dan sejenisnya, serta analisis didukung dengan sumber pustaka primer yang relevan dan terkini.

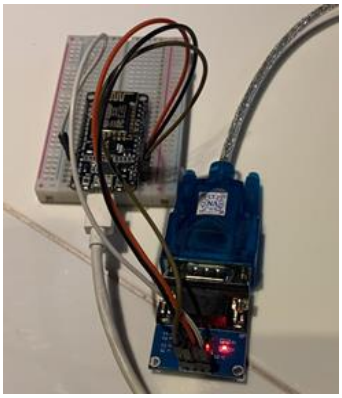
Bagian ini menunjukan proses optimasi keamanan IoT Transaksi Pembayaran dari serangan XSS. Tahap pertama pengumpulan alat penelitian. Tahap kedua perancangan IoT, tahap ketiga pengujian kerentanan sebelum optimasi dilakukan. Tahap keempat implementasi blockchain. Tahap kelima pengujian kerentanan setelah optimasi dilakukan. Alat-alat yang dibutuhkan pada penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Alat Penelitian

No	Nama Alat	Kategori Alat	Keterangan
1	NodeMCU	Hardware	Untuk merancang IoT
2	RS232	Hardware	Untuk merancang IoT
3	Kabel USB	Hardware	Untuk merancang IoT
4	Laptop	Hardware	Untuk merancang IoT
5	XSS Vulnerability Scanner	Software	Untuk Penetration Testing
6	VisualStudio	Software	Untuk merancang Blockchain

Tabel 1 berisi alat penelitian yang dibutuhkan dalam penelitian. NodeMCU, RS232, Kabel USB dan Laptop digunakan untuk merancang IoT. RS232 digunakan untuk mengubah data yang diinputkan oleh pengguna agar bisa dibaca oleh NodeMCU.. XSS Vulnerability Scanner untuk menguji kerentanan IoT transaksi pembayaran dan VisualStudio digunakan untuk merancang blockchain yang akan

diimplementasikan pada IoT transaksi pembayaran. Perancangan IoT transaksi pembayaran digunakan sebagai demonstrasi pengiriman data transaksi *cryptocurrency. Device* diatur agar dapat mengirimkan data melalui sensor yaitu data pengirim, penerima dan nominal amount yang dikirimkan. Perancangan IoT pada penelitian ini dapat dilihat seperti pada Gambar 1.



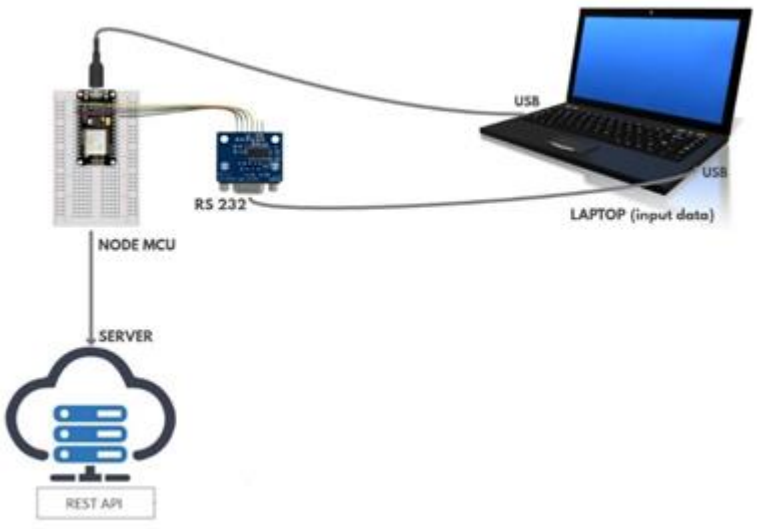
Gambar 1. Perancangan IoT Transaksi Pembayaran

Gambar 1 merupakan gambar RS232 yang dihubungkan dengan NodeMCU menggunakan kabel dengan aturan seperti yang dijelaskan pada Tabel 2.

Table 2. Setting Cable RS232 to NodeMCU

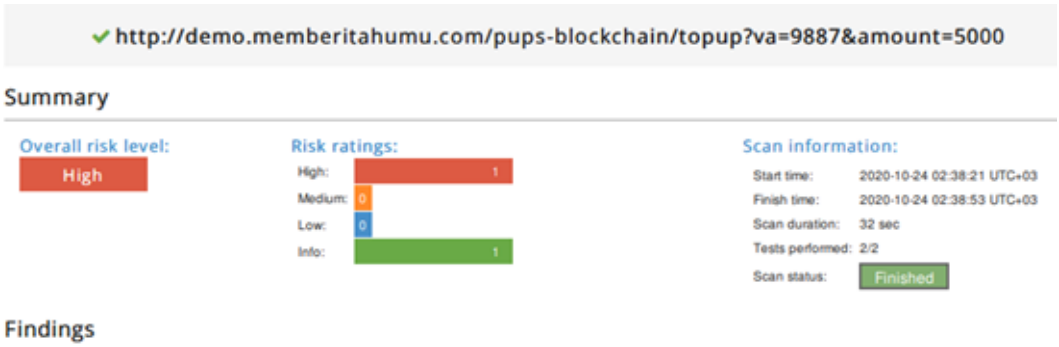
RS232	Dihubungkan	NodeMCU
GND	----------	GND
VCC	----------	3V3
RXD	----------	RX
TXD	----------	TX

Tabel 2 menjelaskan pengaturan kabel untuk menghubungkan RS232 dengan NodeMCU, dimana GND pada RS232 dihubungkan dengan GND pada NodeMCU, VCC dihubungkan dengan 3V3, RDX dengan RX, dan TXD dengan TX. Pengiriman data dari RS232 dapat dilakukan secara satu atau dua arah, kecepatan transfer data cukup rendah maksimal hanya mencapai 19200 bit per sekon. Kemudian untuk rancangan IoT secara lengkap dapat dilihat seperti pada Gambar 2.



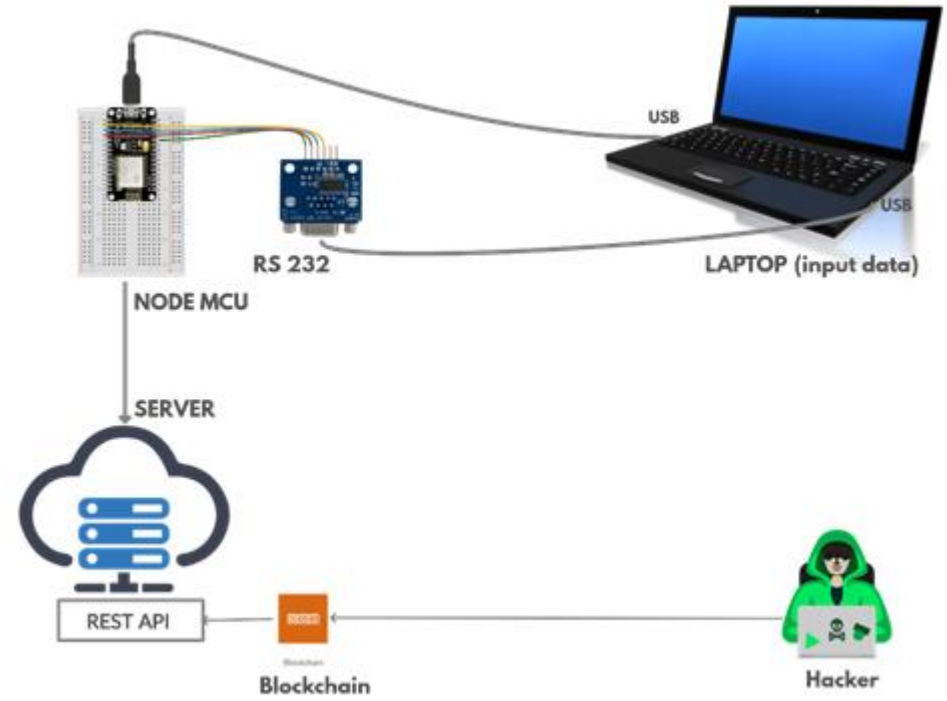
Gambar 2. Perancangan IoT Transaksi Pembayaran

Gambar 2 menunjukan sebuah laptop yang dihubungkan dengan RS232 dan NodeMCU. Laptop digunakan untuk mengirimkan data akun virtual dan ammnout. Data tersebut diterima oleh RS232 untuk diconvert terlebih dahulu, kemudian hasil nya baru dikirimkan ke NodeMCU untuk dilakukan embedded code c++ yang didalamnya terdapat pengaturan data transaksi, url end front Rest API, serta konfigurasi API. Data yang sudah terinstall di dalam NodeMCU langsung bisa dikirimkan ke server. Setelah IoT berhasil dirancang langkah selanjutnya adalah pengujian kerentanan pada IoT tersebut, pengujian kerentanan dilakukan dua kali, pengujian pertama sebelum implementasi blockchain dan pengujian kedua dilakukan sesudah implementasi blockchain. Pengujian kerentanan ini dilakukan menggunakan XSS Vulnerability Scanning, dan hasil dari pengujian kerentanan pertama dapat dilihat pada Gambar 3.



Gambar 3. *Hasil Pengujian Kerentanan*

Gambar 3 menunjukan summary pengujian kerentanan pada webserver demo.memberitahumu.com/pups-blockchain. Laporan dari hasil pengujian kerentanan menunjukan bahwa webserver tersebut memiliki 1 celah kerentanan XSS yang memiliki tingkat risiko keseluruhan berlevel tinggi. Hal ini menunjukan bahwa keamanan pada IoT transaksi pembayaran harus ditingkatkan agar dapat terhindar dari serangan XSS. Langkah selanjutnya adalah implementasi blockchain, yang dilakukan untuk meningkatkan keamanan pada IoT pembayaran yaitu data API yang tersimpan didalam webserver demo.memberitahumu.com/pups-blockchain. Proses implementasi blockchain dapat dilihat seperti pada Gambar 4.



Gambar 4. Implementasi Blockchain

Gambar 4 terlihat bahwa sebuah server REST API yang menerima dan menyimpan data dari IoT transaksi pembayaran menjadi sasaran dari peretas dengan serangan XSS karena pada IoT transaksi pembayaran ditemukan celah kerentanan dari serangan tersebut. Blockchain dirancang untuk mencegah serangan tersebut agar tidak dapat menyerang server REST API. Berikut ini merupakan listing program pada payload REST API sesudah blockchain diimplementasikan.

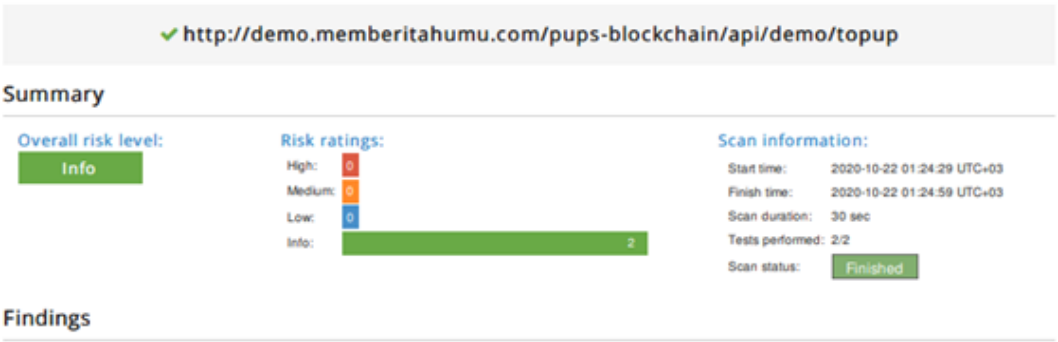
Kode program 4.1 *Form* Registrasi

```
"status": "00",
  "message": "success",
  "name": "Dani Saputra",
  "amount_total": "Rp. 225,000",
  "result": {
       "chain": [

{
"nonce": 0,
"index": 0,
"timestamp": 1587747600,
"data": "Genesis Block",
"previousHash": null,
"hash":"558fdb114cbcef913ed07f45c2f644ea5cabc953eef5884a910195b30742c300"
},
```

```
{
"nonce": 13,
"index": 1,
"timestamp": "1603195046",
"data": "50000",
"previousHash":"558fdb114cbcef913ed07f45c2f644ea5cabc953eef5884a910195b30
742c300",
"hash":"07736a69c442aaf9f78fcf9288c6e94587647c399e643565d6fef4342e71021f"
  },

{
"nonce": 9,
"index": 2,
 "timestamp": "1603197946",
 "data": "75000",
"previousHash":"07736a69c442aaf9f78fcf9288c6e94587647c399e643565d6fef4342
e71021f",
"hash":"0ba9e86bf8644825085d391284baf24c0188da1d9d4203d553bc0b6281ded6a8"
},

{
"nonce": 15,
"index": 3,
 "timestamp": 1603199769,
"data": "100000",
"previousHash":"0ba9e86bf8644825085d391284baf24c0188da1d9d4203d553bc0b628
1ded6a8",
hash":"04f75880b30ed3f9278a83e8648ba1a8b78c567f0e3906b5946a35413a44c03f"
}

],
"difficulty":
“status": "00",
"message": "success",
"name": "Dani Saputra",
"amount_total": "Rp. 225,000",
"result": [

{
"amount": "50000"
},
{
"amount": "75000"
},
{
"amount": "100000"
}
]

}
```


Data yang dikirimkan berupa nama dan jumlah uang yang kemudian dijadikan sebuah blok. Setiap blok pada blockchain berisi timestamp, data, previous hash, dan hash itu sendiri. Blok pertama disebut dengan blok genesis, berisi data transaksi dengan previous hash yang masih null dan menghasilkan hash untuk blok itu sendiri, begitu juga dengan blok selanjutnya, hanya saja yang membedakan adalah isi dari previous hash nya sudah tidak null lagi dan nilai hash masing-masing blok. Data transaksi pembayaran yang diinputkan oleh pengguna dapat dilihat dan dibaca oleh semua anggota yang terhubung dalam jaringan blockchain. Implementasi

blockchain akan disingkronkan terhadap semua data transaksi pembayaran yang dilakukan oleh device IoT. Setiap anggota pada jaringan blockchain masing-masing memiliki key pair untuk dapat melakukan transaksi. Setiap data yang diinputkan menjadi sebuah blok yang saling terhubung satu sama lain menjadi sebuah rantai/chain, maka dari itu setiap anggota tidak diperkenankan untuk mengubah atau menghapus setiap blok data. Rantai yang berisi blok blok yang saling terhubung akan dilakukan consesus agar blok yang berisi data tidak valid bisa diabaikan oleh anggota lain bahkan dihapus dari jaringan blockchain secara otomatis. Setiap blok dengan nilai transaksi yang berbeda dengan nilai mayoritas dalam suatu jaringan blockchain akan dieliminasi dan dilakukan perbaikan kembali kenilai yang telah tersimpan pada setiap data anggota blockchain, maka dari itu apabila ada penyerang yang mencoba mengubah data transaksi pada jaringan blockchain tersebut akan dieliminasi dan data yang sudah diubah akan diperbaiki secara otomatis. Langkah terakhir yang dilakukan adalah pengujian kerentanan dilakukan kembali sesudah implementasi blockchain dilakukan, hal ini bertujuan untuk membuktikan apakah implementasi blockchain untuk meningkatkan IoT transaksi pembayaran berhasil dilakukan. Hasil dari pengujian kerentanan ini dapat dilihat pada Gambar 5.



Gambar 5. Hasil Pengujian Kerentanan setelah Implementasi Blockchain

Gambar 5 menunjukan hasil pengujian kerentanan setelah implementasi blockchain dilakukan, hasil dari pengujian kerentanan tersebut menunjukan tingkat risiko secara keseluruhan adalah tidak ditemukannya kerentanan dari serangan XSS, hal

ini menunjukan bahwa optimasi keamanan IoT transaksi pembayaran dengan menggunakan blockchain 100% berhasil dilakukan.

D. STATUS LUARAN: Tuliskan jenis, identitas dan status ketercapaian setiap luaran wajib dan luaran tambahan (jika ada) yang dijanjikan pada tahun pelaksanaan penelitian. Jenis luaran dapat berupa publikasi, perolehan kekayaan intelektual, hasil pengujian atau luaran lainnya yang telah dijanjikan pada proposal. Uraian status luaran harus didukung dengan bukti kemajuan ketercapaian luaran sesuai dengan luaran yang dijanjikan. Lampirkan pada laporan akhir bukti dokumen ketercapaian luaran wajib dan luaran tambahannya.

	Keterangan
ARTIKEL JURNAL KE-1	**Blockchain Could Secure XSS Attack**
Nama jurnal yang dituju	Journal of Engineering Science and Technology (JESTEC)
Level jurnal	Internasional
Status	Bereputasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit - In Review
Alamat URL artikel	http://jestec.taylors.edu.my/
ARTIKEL JURNAL KE-2	**Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain**
Nama jurnal yang dituju	JIEET (Journal of Information Engineering and Educational Technology)
Level jurnal	Nasional
Status	Terakreditasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Published
Alamat URL artikel	https://journal.unesa.ac.id/index.php/jieet
ARTIKEL JURNAL KE-3	**Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology Modification**
Nama jurnal yang dituju	Lontar Komputer
Level jurnal	Nasional
Status	Terakreditasi
Impact factor untuk jurnal	

Judul artikel	
Status naskah	Accepted
Alamat URL artikel	https://ojs.unud.ac.id/index.php/lontar
ARTIKEL JURNAL KE-4	**Image Forensic with Digital Forensic Research Workshop Method Internet of thing (IoT) security optimization against cross-site scripting (XSS) attacks based on blockchain technology**
Nama jurnal yang dituju	KINETIK
Level jurnal	Nasional
Status	Bereputasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	https://kinetik.umm.ac.id/index.php/kinetik/
ARTIKEL JURNAL KE-5	**Optimization Security on Internet of Things from Broken Authentication Attack using Blockchain Technology**
Nama jurnal yang dituju	IEEE Access
Level jurnal	International
Status	Terakreditasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	https://ieeexplore.ieee.org/
ARTIKEL JURNAL KE-6	**A Framework for Securing Covid-19 Data in Electronic Health Record against SQL Injection using Blockchain Technology**
Nama jurnal yang dituju	CST Kipmi
Level jurnal	International
Status	Terakreditasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	https://cst.kipmi.or.id/journal

E. PERAN MITRA: Tuliskan realisasi kerjasama dan kontribusi Mitra baik *in-kind* maupun *in-cash* (jika ada). Bukti pendukung realisasi kerjasama dan realisasi kontribusi mitra dilaporkan sesuai dengan kondisi yang sebenarnya. Bukti dokumen realisasi kerjasama dengan Mitra dilampirkan di dalam laporan akhir.

Penelitian ini bekerja sama dengan ATT CDV (AMNOTEL Cyber Digital Valley). Kontribusi mitra diantaranya adalah menyediakan tempat untuk melakukan implementasi penelitian, didukung dengan koneksi internet dan listrik.

F. KENDALA PELAKSANAAN PENELITIAN: Tuliskan kesulitan atau hambatan yang dihadapi selama melakukan penelitian dan mencapai luaran yang dijanjikan, termasuk penjelasan jika pelaksanaan penelitian dan luaran penelitian tidak sesuai dengan yang direncanakan atau dijanjikan.

Kendala yang kami dapatkan selama melakukan penelitian adalah adanya pandemi Covid-19 yang membuat proses diskusi lebih sering dilakukan secara *online*, sehingga ketika ada permasalahan koneksi buruk, maka diskusi menjadi tidak efektif. Teknologi Blockchain ini masih dibilang baru di Indonesia, sumber-sumber referensi ilmu terkait bidang ini masih sulit kami temui dari orang Indonesia sehingga pemahaman akan teknologi ini masih terbatas dan kesulitan melakukan implementasi. Atas beberapa kendala tersebut beberapa target luaran menjadi terhambat dan harus diselesaikan pada tahap selanjutnya.

G. RENCANA TINDAK LANJUT PENELITIAN: Tuliskan dan uraikan rencana tindak lanjut penelitian selanjutnya dengan melihat hasil penelitian yang telah diperoleh. Jika ada target yang belum diselesaikan pada akhir tahun pelaksanaan penelitian, pada bagian ini dapat dituliskan rencana penyelesaian target yang belum tercapai tersebut.

Setelah satu tahun melakukan riset teknologi Blockchain, kami mendapatkan pemahaman baru tentang apa itu Blockchain. Kami menemukan sebuah Blockchain yang bersifat *open source* yaitu ethereum, dimana kita bisa melakukan eksplorasi teknologi ini. Salah satunya adalah *smart contract* yang memang menjadi tujuan utama dibuatnya ethereum. Banyak target yang belum kami selesaikan di antaranya luaran masih pada tahap *submitted* dan revisi dari reviewer, kami akan menyelesaikan target luaran tersebut hingga pada tahap *accepted paper*. Rencana lain adalah kami berupaya melakukan riset lebih dalam tentang *smart contract*,

beberapa ide sudah kami dapatkan terkait *smart contract* dan *internet of things* ini. Riset ini tidak hanya melakukan implementasi *smart contract* pada IoT saja, namun upaya mengamankan *smart contract* tersebut dari berbagai *vulnerability* yang mungkin terjadi.

H. DAFTAR PUSTAKA:

Arief, L., Andalas, U. and Sundara, T. (2017) 'Studi atas Pemanfaatan Blockchain bagi Internet of Things (IoT)', (August). doi: 10.29207/resti.v1i1.26.

Akbar, M. 21 Januari 2019. Cross Site Scripting: Dasar – Dasar Xss. Ditemukenali 30 Januari 2020, dari https://abaykan.com/cross-site-scripting-dasar/

Dewaweb Team. 3 Agustus 2018. Internet of Things: Panduan Lengkap. Ditemukenali 30 Januari 2020, dari https://www.dewaweb.com/blog/internet-of-things/

Dolorosa, M. et al. (2018) 'Blockchain Untuk Keamanan Transaksi Elektronik Perusahaan Financial Technology (Studi Kasus Pada Pt Xyz)', pp. 7–12.

Kurniawan, M. R. Et al. 1 Juli 2013. Tentang Cross Site Scripting. Ditemukenali 30 Januari 2020, dari https://yusniaalfisyahrin.wordpress.com/2013/07/01/tentang-cross-site-scripting/

Kpu, P. (2019) 'Blockchain Pada Sistem Pencatatan Hasil Rekapitulasi Pemilu Berdasarkan Formulir C1 Dwi Fitra Hidayat Satria Wibowo NIM : 23217053 (Program Studi Magister Teknik Elektro) Institut Teknologi Bandung Februari 2019 Abstrak Rekapitulasi Pemilu Berdasarkan F', 23217053.

Putra, G. D. and Sumaryono, S. (2018) 'Rancang Bangun Identity and Access Management IoT Berbasis KSI dan Permissioned Blockchain', 7(4), pp. 384–390.

Permana, Y. 25 Februari 2019. Penjelasan Sederhana mengenai Internet of Things. Ditemukenali 30 Januari 2020, dari https://www.codepolitan.com/apa-sih-yang-dimaksud-internet-of-thing

Rakha, R. et al. (2018) 'Kesehatan Untuk Pendeteksian Fraud (Studi Kasus : Bpjs Kesehatan)', (November).

Satuti, W. S. 27 Agustus 2019. Mengenal Blockchain, Keunggulan, Cara Kerja, dan Karakter. Ditemukenali 30 Januari 2020, dari https://jojonomic.com/blog/blockchain/

LAMPIRAN 1

(Salinan Kontrak)

PERGURUAN TINGGI MUHAMMADIYAH
UNIVERSITAS AHMAD DAHLAN
LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
Jalan Gondosuli 1B Semaki, Yogyakarta 55166 Telp. (0274) 542886, Fax. (0274) 542886

SURAT PERJANJIAN PELAKSANAAN PENELITIAN

Nomor: PUPS-013/SP3/LPPM-UAD/2020

Pada hari ini, **Sabtu** tanggal **Delapan belas** bulan **April** tahun **Dua ribu dua puluh (18-04-2020)**, kami yang bertandatangan di bawah ini:

1. Nama : **Dr. Widodo, M.Si.**
   Jabatan : Kepala Lembaga Penelitian dan Pengabdian Kepada Masyarakat Universitas Ahmad Dahlan (LPPM UAD), selanjutnya disebut sebagai **PIHAK PERTAMA.**
2. Nama : **IMAM RIADI. Dr.. M.Kom**
   Jabatan : Dosen/Peneliti pada Program Studi **Sistem Informasi Fakultas Sain dan Teknologi Terapan (FAST)** Universitas Ahmad Dahlan (UAD), selaku Ketua Peneliti, selanjutnya disebut **PIHAK KEDUA.**

Kedua belah pihak menyatakan setuju dan mufakat untuk mengadakan perjanjian pelaksanaan penelitian untuk selanjutnya disebut Surat Perjanjian Pelaksanaan Penelitian (SP3) dengan ketentuan dan syarat-syarat sebagai berikut.

Pasal 1

DASAR HUKUM

(1) Hasil review/penilaian proposal yang dilakukan oleh Tim Reviewer Penelitian Internal UAD.

(2) Surat Keputusan Kepala LPPM UAD nomor: L1/098/L0/IV/2020 tanggal 15 April 2020 tentang Penetapan Hasil Seleksi Proposal Penelitian Dana UAD Tahun Akademik 2019/2020.

Pasal 2

RUANG LINGKUP

(1) PIHAK PERTAMA memberikan pekerjaan kepada PIHAK KEDUA dan PIHAK KEDUA menyatakan menerima pekerjaan dari PIHAK PERTAMA berupa kegiatan penelitian sebagai berikut.

Skema	:	Penelitian Unggulan Program Studi (PUPS)
Judul penelitian	:	Optimasi Keamanan IoT Terhadap Serangan Cross Site Scripting (XSS) Menggunakan Teknologi Blockchain
Jenis Riset	:	Riset Terapan (RT) , TKT: 5
Mitra Penelitian	:	ATTCDV (Amnotel Cyber Digital Valley)
Luaran Wajib	:	Artikel pada Jurnal

(2) Jangka waktu penelitian tersebut pada ayat (1) paling lama **6 (enam) bulan** sejak ditandatangani SP3 ini, dan menyerahkan hasil laporan penelitian sementara kepada PIHAK PERTAMA selambat-lambatnya pada **18 Oktober 2020.**

(3) PIHAK KEDUA berkewajiban untuk merealisasikan luaran penelitian seperti yang dijanjikan dalam proposal penelitian.

Pasal 3

PERSONALIA PELAKSANA PENELITIAN

Personalia pelaksana penelitian ini terdiri dari:

Ketua Peneliti	: IMAM RIADI. Dr.. M.Kom
Pembimbing	
Anggota 1	: RUSYDI UMAR. S.T.. M.T.. P.hD.
Anggota 2	: -

Paraf: .....

Pasal 4

BIAYA PENELITIAN DAN CARA PEMBAYARAN

(1) PIHAK PERTAMA menyediakan dana pelaksanaan penelitian kepada PIHAK KEDUA sejumlah **Rp 20,000,000,00 (Duabelas Juta rupiah)** yang dibebankan pada Anggaran Pendapatan dan Belanja (APB) LPPM UAD Tahun Akademik 2019/2020 dibayarkan melalui rekening bank atas nama Ketua Peneliti oleh Bidang Finansial UAD sebagai berikut.

Nama : IMAM RIADI. Dr., M.Kom
Nama Bank : BPD DIY SYARIAH
Nomor rekening : 801,211,007,876

(2) **Tahap I sebesar 60% x Rp 20,000,000,00 = Rp 12,000,000,00** (Duabelas Juta rupiah), dibayarkan setelah SP3 ini ditandatangani oleh PARA PIHAK dan PIHAK KEDUA telah mengunggah file scan SP3 ini pada portal UAD selambat-lambatnya pada Juni 2020.

(3) **Tahap II sebesar 40% x Rp 20,000,000,00 = Rp 8,000,000,00** (Delapan Juta rupiah), dibayarkan setelah: (a) PIHAK KEDUA mengunggah revisi laporan akhir pasca kolokium dan (b) luaran wajib penelitian telah submit (minimal) untuk jenis luaran jurnal/seminar, atau tersedia draft untuk jenis luaran buku/naskah akademik, atau telah mendaftarkan kekayaan intelektual (KI) untuk jenis luaran paten dan hak cipta dan jenis KI lainnya, dan sejenisnya.

Jika PIHAK KEDUA hanya melakukan poin (a) sedangkan poin (b) TIDAK TERPENUHI, maka dana penelitian tahap II hanya dapat dicairkan sebesar 20%.

Pasal 5

PELAKSANAAN PEMBIMBINGAN

(1) Khusus skema Penelitian Dosen Pemula (PDP), peneliti wajib melakukan pembimbingan atau konsultasi dengan dosen pembimbing penelitiannya paling sedikit 4 (empat) kali pembimbingan.

(2) Pembimbingan sebagaimana dimaksud dalam ayat (1) minimal dalam hal-hal sebagai berikut.
a. penyusunan angket/kuesioner dan atau teknik pengumpulan data lainnya;
b. analisis data dan interpretasinya;
c. penyusunan hasil penelitian, pembahasan, penarikan kesimpulan;
d. penyusunan luaran penelitian.

(3) Pembimbingan sebagaimana dimaksud dalam ayat (1) dan ayat (2) dituliskan dalam form pembimbingan yang ditandatangani oleh peneliti dan dosen pembimbing penelitian.

Pasal 6

JENIS LAPORAN PENELITIAN

(1) PIHAK KEDUA wajib menyusun dan menyampaikan laporan penelitian baik secara *on line* melalui portal UAD maupun *hardcopy* kepada PIHAK PERTAMA yang terdiri atas:
a. Laporan Kemajuan
b. Laporan Sementara
b. Laporan Akhir Penelitian

(2) Berkas **Laporan Kemajuan** digunakan sebagai bahan monitoring dan evaluasi (monev) internal.

(3) Berkas **Laporan Sementara** digunakan sebagai bahan kolokium laporan penelitian.

(4) Berkas **Laporan Akhir Penelitian** merupakan revisi dari Laporan Penelitian Sementara pasca kolokium.

Paraf: .....

Pasal 7

MONITORING DAN EVALUASI

(1) PIHAK PERTAMA berhak untuk melakukan monitoring dan evaluasi (monev) internal pelaksanaan penelitian, baik secara administrasi maupun substansi.

(2) Pemantauan kemajuan penelitian dilakukan oleh Tim Monev yang dibentuk oleh PIHAK PERTAMA.

(3) PIHAK KEDUA diharuskan MENYIAPKAN SEMUA DOKUMEN/BUKTI kemajuan pelaksanaan penelitiannya guna kepentingan monev.

(4) Waktu pelaksanaan monev akan ditentukan oleh PIHAK PERTAMA.

Pasal 8

KOLOKIUM LAPORAN PENELITIAN

(1) PIHAK KEDUA wajib menyerahkan **Laporan Penelitian Sementara** sebagai bahan kolokium selambat-lambatnya **18 Oktober 2020.**

(2) Ketua Peneliti wajib hadir dan mempresentasikan hasil penelitiannya pada kolokium **Laporan Penelitian Sementara** yang pelaksanaannya akan diatur oleh PIHAK PERTAMA.

(3) Revisi laporan penelitian yang sudah dikolokiumkan harus mendapatkan pengesahan dari reviewer dalam bentuk **Surat Pernyataan** dan dijilid dalam satu kesatuan laporan penelitian.

Pasal 9

LAPORAN AKHIR PENELITIAN

(1) PIHAK KEDUA wajib menyerahkan **Laporan Akhir Penelitian** selambat-lambatnya **2 (dua) pekan** setelah dikolokiumkan.

(2) Penyusunan laporan penelitian mengacu pada ketentuan dalam Pedoman Penelitian yang dikeluarkan oleh LPPM dan ketentuan lain yang berlaku.

(3) Laporan Akhir Penelitian sebagaimana tersebut pada ayat (1) dan (2) harus memenuhi ketentuan sebagai berikut:
a. bentuk/ukuran kertas A4;
b. warna cover sesuai ketentuan;
c. di bawah bagian cover ditulis:

PENELITIAN INI DILAKSANAKAN ATAS BIAYA
ANGGARAN PENDAPATAN DAN BELANJA UNIVERSITAS AHMAD DAHLAN
TAHUN AKADEMIK 2019/2020
NOMOR KONTRAK: PUPS-013/SP3/LPPM-UAD/2020

(4) PIHAK KEDUA wajib mengunggah file laporan akhir penelitian secara lengkap pada alamat http://www.simpel.uad.ac.id melalui akun portal ketua peneliti dengan format file PDF.

Pasal 10

TANGGUNGAN PENELITIAN DAN LUARAN PENELITIAN

(1) Peneliti dinyatakan memiliki **tanggungan atau hutang penelitian** apabila sampai pada masa penerimaan proposal penelitian periode berikutnya belum menyelesaikan kewajibannya.

(2) Peneliti yang memiliki tanggungan penelitian sebagaimana dimaksud pada ayat (1) tidak diperkenankan mengajukan proposal penelitian pada periode tersebut.

(3) Peneliti dinyatakan memiliki **tanggungan atau hutang luaran penelitian** apabila sampai pada masa pengumpulan revisi laporan akhir penelitian pasca kolokium target luaran wajib penelitiannya belum submit (minimal) untuk jurnal/seminar, atau tersedia draft buku/naskah akademik, atau mendaftarkan kekayaan intelektual (KI), dan sejenisnya.

Paraf: .....

(4) Peneliti yang memiliki tanggungan luaran penelitian sebagaimana dimaksud pada ayat (3) masih diperkenankan mengajukan proposal penelitian pada periode tersebut.

(5) Peneliti yang belum memenuhi luaran wajib berupa *accepted* (minimal) untuk jurnal/seminar, atau terbit buku/naskah akademik, atau tersedia sertifikat kekayaan intelektual (KI), dan sejenisnya selama dua periode penelitian berturut, tidak diperkenankan mengajukan proposal penelitian pada periode tersebut.

Pasal 11

SANKSI DAN PEMUTUSAN PERJANJIAN PENELITIAN

(1) PIHAK PERTAMA berhak memberikan peringatan dan atau teguran atas kelalaian dan atau pelanggaran yang dilakukan oleh PIHAK KEDUA yang mengakibatkan tidak dapat terpenuhinya kontrak penelitian ini.

(2) PIHAK PERTAMA berhak melakukan pemutusan perjanjian penelitian, jika PIHAK KEDUA tidak mengindahkan peringatan yang diberikan oleh PIHAK PERTAMA.

(3) Segala kerugian material maupun finansial yang disebabkan akibat kelalaian PIHAK KEDUA, maka sepenuhnya menjadi tanggungjawab PIHAK KEDUA.

(4) Jenis sanksi yang diberikan dapat berupa:
   (a) tidak diperkenankannya mengajukan proposal penelitian sebagaimana dimaksud pada Pasal 10 ayat (5) sampai kewajibannya terselesaikan; dan atau
   (b) tidak dapat mencairkan dana tahap 2; dan atau
   (c) mengembalikan dana yang telah diterima oleh PIHAK KEDUA.

Pasal 12

KEADAAN MEMAKSA (*FORCE MAJEUR*)

Ketentuan dalam Pasal 10 tersebut di atas tidak berlaku dalam keadaan sebagai berikut:

a. Keadaan Memaksa (*force majeur*)

b. PIHAK PERTAMA menyetujui atas terjadinya keterlambatan yang didasarkan pada pemberitahuan sebelumnya oleh PIHAK KEDUA kepada PIHAK PERTAMA dengan **surat pemberitahuan** mengenai kemungkinan terjadinya keterlambatan dalam penyelesaian kegiatan penelitian sebagaimana dimaksud dalam Pasal 1 dan Pasal 3; dan sebaliknya PIHAK KEDUA menyetujui terjadinya keterlambatan pembayaran sebagai akibat keterlambatan dalam penyelesaian perjanjian penelitian.

Pasal 13

(1) Keadaan Memaksa (*force majeur*) sebagaimana yang dimaksud dalam Pasal 12 ayat (1) adalah peristiwa-peristiwa yang secara langsung mempengaruhi pelaksanaan perjanjian serta terjadi di luar kekuasaan dan kemampuan PIHAK KEDUA ataupun PIHAK PERTAMA.

(2) Peristiwa yang tergolong dalam keadaan memaksa (*force majeur*) antara lain berupa bencana alam, pemogokan, wabah penyakit, huru-hara, pemberontakan, perang, waktu kerja diperpendek oleh pemerintah, kebakaran dan atau peraturan pemerintah mengenai keadaan bahaya serta hal-hal lainnya yang dipersamakan dengan itu, sehingga PIHAK KEDUA ataupun PIHAK PERTAMA terpaksa tidak dapat memenuhi kewajibannya.

(3) Peristiwa sebagaimana dimaksud pada ayat (2) tersebut di atas, wajib diberikan oleh penguasa setempat dan diberitahukan dengan Surat oleh PIHAK KEDUA atau PIHAK PERTAMA kepada PIHAK PERTAMA atau PIHAK KEDUA selambat-lambatnya 7 (tujuh) hari sejak terjadinya peristiwa yang dikategorikan sebagai Keadaan Memaksa (*force majeur*).

(4) PIHAK PERTAMA memberikan kesempatan kepada PIHAK KEDUA untuk menyelesaikan perjanjian kontrak ini sampai pada batas waktu yang disepakati oleh kedua belah pihak jika keadaan *force majeur* dinyatakan telah selesai.

Paraf: .....

Pasal 14

PENYELESAIAN PERSELISIHAN

(1) Apabila dalam pelaksanaan perjanjian dan segala akibatnya timbul perbedaan pendapat atau perselisihan, PIHAK PERTAMA dan PIHAK KEDUA setuju untuk menyelesaikannya secara musyawarah untuk mencapai mufakat.

(2) Apabila penyelesaian sebagaimana termaksud dalam ayat (1) di atas tidak tercapai, maka PIHAK PERTAMA dan PIHAK KEDUA sepakat menyerahkan perselisihan tersebut melalui mediasi dengan Rektor sebagai atasan langsung dari PIHAK PERTAMA yang putusannya bersifat final dan mengikat.

Pasal 15

PENGUNDURAN DIRI

(1) Apabila PIHAK KEDUA mengundurkan diri atau membatalkan SP3 ini, maka PIHAK KEDUA wajib mengajukan Surat Pengunduran Diri yang ditujukan kepada PIHAK PERTAMA.

(2) Surat Pengunduran Diri sebagaimana dimaksud pada ayat (1) wajib disahkan oleh Dekan fakultas ketua peneliti yang bersangkutan; dan bagi peneliti skim PDP ditambah persetujuan Dosen Pembimbing.

(3) PIHAK KEDUA wajib mengembalikan dana yang telah diterima kepada PIHAK PERTAMA

Pasal 16

LAIN-LAIN

(1) Hal-hal yang dianggap belum cukup dan perubahan-perubahan perjanjian akan diatur kemudian atas dasar permufakatan kedua belah pihak yang akan dituangkan dalam bentuk Surat atau Perjanjian Tambahan (addendum), yang merupakan kesatuan dan bagian yang tidak terpisahkan dari perjanjian awal.

(2) Surat Perjanjian Pelaksanaan Penelitian (SP3) ini berlaku sejak ditandatangani dan disetujui oleh kedua belah pihak.

PIHAK PERTAMA,

Dr. Widodo, M.Si.
NIP. 19600221198709101

PIHAK KE DUA,

IMAM RIADI, Dr., M.Kom
NIP/NIY. 60020397

Paraf: .....

LAMPIRAN 2

(Borang Capaian Luaran Penelitian)

BORANG CAPAIAN LUARAN PENELITIAN
SUMBERDANA UAD TAHUN AKADEMIK 2019/2020
SKEMA PENELITIAN UNGGULAN PROGRAM STUDI

I. IDENTITAS PENELITI

Judul penelitian : Optimasi Keamanan IoT terhadap Serangan Cross Site Scripting (XSS) Menggunakan Teknologi Blockchain
Ketua Peneliti : Dr. Imam Riadi, M.Kom
NIDN / e-mail : 0510088001/riadi@is.uad.ac.id
Prodi/Fakultas : Sistem Informasi/Sains dan Teknologi Terapan
Anggota Peneliti 1 : Rusydi Umar, S.T., M.T., Ph.D
Jenis/Tahap Penelitian : Pengembangan
TKT/TRL :

II. CAPAIAN LUARAN PENELITIAN

A. PUBLIKASI ILMIAH

	Keterangan
ARTIKEL JURNAL KE-1	**Blockchain Could Secure XSS Attack**
Nama jurnal yang dituju	Journal of Engineering Science and Technology (JESTEC)
Level jurnal	Internasional
Status	Bereputasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit - In Review
Alamat URL artikel	http://jestec.taylors.edu.my/
ARTIKEL JURNAL KE-2	**Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain**
Nama jurnal yang dituju	JIEET (Journal of Information Engineering and Educational Technology)
Level jurnal	Nasional
Status	Terakreditasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Published
Alamat URL artikel	https://journal.unesa.ac.id/index.php/jieet
ARTIKEL JURNAL KE-3	**Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology Modification**
Nama jurnal yang dituju	Lontar Komputer
Level jurnal	Nasional
Status	Terakreditasi

Impact factor untuk jurnal	
Judul artikel	
Status naskah	Accepted
Alamat URL artikel	https://ojs.unud.ac.id/index.php/lontar
ARTIKEL JURNAL KE-4	**Image Forensic with Digital Forensic Research Workshop Method Internet of thing (IoT) security optimization against cross-site scripting (XSS) attacks based on blockchain technology**
Nama jurnal yang dituju	KINETIK
Level jurnal	Nasional
Status	Bereputasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	https://kinetik.umm.ac.id/index.php/kinetik/
ARTIKEL JURNAL KE-5	**Optimization Security on Internet of Things from Broken Authentication Attack using Blockchain Technology**
Nama jurnal yang dituju	IEEE Access
Level jurnal	International
Status	Terakreditasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	https://ieeexplore.ieee.org/
ARTIKEL JURNAL KE-6	**A Framework for Securing Covid-19 Data in Electronic Health Record against SQL Injection using Blockchain Technology**
Nama jurnal yang dituju	CST Kipmi
Level jurnal	International
Status	Terakreditasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	https://cst.kipmi.or.id/journal

B. BUKU AJAR

Buku ke-1*[2]	**Keterangan**
Judul buku	
Penulis	

Penerbit	
No. ISBN	
Buku ke-2, dst.	

*[2] Jika masih ada buku ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

C. PEMBICARA PADA PERTEMUAN ILMIAH (SEMINAR/SIMPOSIUM)

Mengikuti seminar*[3]	**Keterangan**
Pertemuan Ilmiah ke-1	
- Judul Makalah	
- Nama pertemuan ilmiah	
- Tempat pelaksanaan	
- Waktu pelaksanaan	
- Jenis pertemuan	
- Status naskah	
Pertemuan Ilmiah ke-2, dst.	

*[3] Jika masih ada undangan ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

D. PEMBICARA KUNCI/*KEYNOTE* SPEAKER PADA PERTEMUAN ILMIAH (SEMINAR/SIMPOSIUM)

	Keterangan
- Judul makalah	
- Penulis	
- Penyelenggara	
- Waktu Pelaksanaan	
- Tempat Pelaksanaan	
- Skala pertemuan	Regional/Nasional/Internasional
- Status pertemuan	Sudah dilaksanakan / belum
- Alamat URL artikel	
-	

*[3] Jika masih ada undangan ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

E. Menjadi Peneliti Tamu (*Visiting Scientist)*

Menjadi peneliti tamu (*visiting scientist*) pada perguruan tinggi lain*[4]	**Nasional**	**Internasional**
- Perguruan tinggi pengundang		
- Lama kegiatan		
- Kegiatan penting yang dilakukan		

*[4] Jika masih ada undangan ke-2 dan seterusnya, mohon dituliskan pada lembar tambahan

F. Hak Kekayaan Intelektual dan Lainnya

Jenis HKI	Uraian
Paten	Tuliskan judul paten adan tanggal pengajuannya
Hak Cipta	Tuliskan bentuk dan atau nama/judul hak cipta dan tanggal pengajuannya
TEKNOLOGI TEPAT GUNA	Jelaskan nama TTG dan pemanfaatan serta penggunanya
REKAYASA SOSIAL	Uraikan kebijakan publik yang sedang atau sudah dapat diubah
JEJARING KERJA SAMA	Uraikan kapan jejaring dibentuk dan kegiatannya sampai saat ini, baik antarpeneliti maupun antarlembaga
PENGHARGAAN	Uraikan penghargaan yang diterima sebagai peneliti, baik dari pemerintah atau asosiasi profesi
LAINNYA	Tulis dan uraikan luaran HKI lainnya

Yogyakarta, 31 Oktober 2019
Ketua Peneliti,

Sunardi, S.T., M.T., Ph.D

LEMBAR TAMBAHAN

	Keterangan
ARTIKEL JURNAL KE-2	**Audio Forensic on Smartphone with Digital Forensic Research Workshop Method (DFRWS)**
Nama jurnal yang dituju	IGI Global International Journal of Technoethics (IJT)
Level jurnal	Internasional
Status	Bereputasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	https://www.igi-global.com/
ARTIKEL JURNAL KE-3	**FORENSIK MOBILE PADA SMARTPHONE ANDROID MENGGUNAKAN METODE DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS)**
Nama jurnal yang dituju	Jurnal Penelitian Pos dan Informatika (JPPI)
Level jurnal	Nasional
Status	Terakreditasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	jurnal-ppi.kominfo.go.id
ARTIKEL JURNAL KE-4	Analisis Perbandingan *Tools* Forensik Metode
Nama jurnal yang dituju	Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)
Level jurnal	Nasional
Status	Terakreditasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	http://www.jurnal.iaii.or.id/index.php/RESTI
ARTIKEL JURNAL KE-5	Image Forensic with *Digital Forensic Research Workshop* Method
Nama jurnal yang dituju	IGI GLOBAL Internasional journal of digital crime and forensics
Level jurnal	Internasional
Status	Bereputasi
Impact factor untuk jurnal	
Judul artikel	
Status naskah	Submit
Alamat URL artikel	https://www.igi-global.com/

LAMPIRAN 3

(Profil Penelitian)

LAMPIRAN 4

(Presensi Kolokium)

LAMPIRAN 5

(Personalia Peneliti)

PERSONALIA PENELITIAN

Judul Penelitian :Optimasi Keamanan IoT terhadap Serangan *Cross Site Scripting* (XSS) Menggunakan Teknologi *Blockchain*

Skema : Penelitian Unggulan Program Studi

1. Ketua Peneliti

a. Nama Lengkap dan Gelar : Dr. Imam Riadi, M.Kom.
b. NIDN/NIY/NIP : 0510088001 / 60020397
c. Fakultas/Program Studi : Sains dan Teknologi Terapan/Sistem Informasi
d. Jabatan Akademik : Lektor Kepala
e. Alokasi waktu untuk penelitian : 6 Bulan
f. Tugas dalam penelitian : 1. Koordinasi team work

2. Anggota Peneliti 1

a. Nama Lengkap dan Gelar : Rusydi Umar, S.T., M.T., Ph.D
b. NIDN/NIY/NIP : 60980174 / 0507087202
c. Fakultas/Program Studi : Teknologi Industri/Magister Teknik Informatika
d. Jabatan Akademik : Lektor
e. Alokasi waktu untuk penelitian : 6 Bulan
f. Tugas dalam penelitian : 1. Koordinasi team work

3. Keterlibatan Mahasiswa

No	Nama Mahasiswa dan NIM	Program Studi	Tugas dalam Tim	Judul Tugas Akhir
1	Tri Lestari NIM: 1907048008	Magister Teknik Informatika	Penulisan Jurnal	Optimasi Keamanan IoT dari Serangan XSS Berbasis Teknologi Blockchain
2	Iqbal Busthomi NIM: 1907048011	Magister Teknik Informatika	Penulisan Jurnal	Optimasi Keamanan Informasi Terhadap Serangan Man in the Middle (MiTM) Menggunakan Teknologi Blockchain
3	Achmad Nugrahantoro NIM: 1907048001	Magister Teknik Informatika	Penulisan Jurnal	Keamanan RESTful Web Service Menggunakan Jaringan Syaraf Tiruan (JST) dan Advanced Encryption Standard (AES)

	M. Nasir Hafizh NIM: 1907048019	Magister Teknik Informatika	Penulisan Jurnal	Analisis Perbandingan Metode Backpropagation dan Adaptive Neuro Fuzzy Inference System untuk Prediksi Curah Hujan
	Purwono NIM: 1907048015	Magister Teknik Informatika	Penulisan Jurnal	Image Forensik untuk Mendeteksi Image Forgery Pada Foto Digital

LAMPIRAN 6

(Bukti Submit)

Your Manuscript ID EE20282 /New Submission, some issues found/

Inbox ×

Jestec <Jestec@taylors.edu.my> Sat, Sep 19, 2020, 5:50 PM

to me

Dear Author,

Thank you for submitting your research paper to the Journal of Engineering Science and Technology (JESTEC).

Kindly note that we have received the paper entitled

BLOCKCHAIN COULD SECURE XSS ATTACK

Your paper ID is EE20282 *(Please quote the above manuscript ID in all future correspondence with us)*

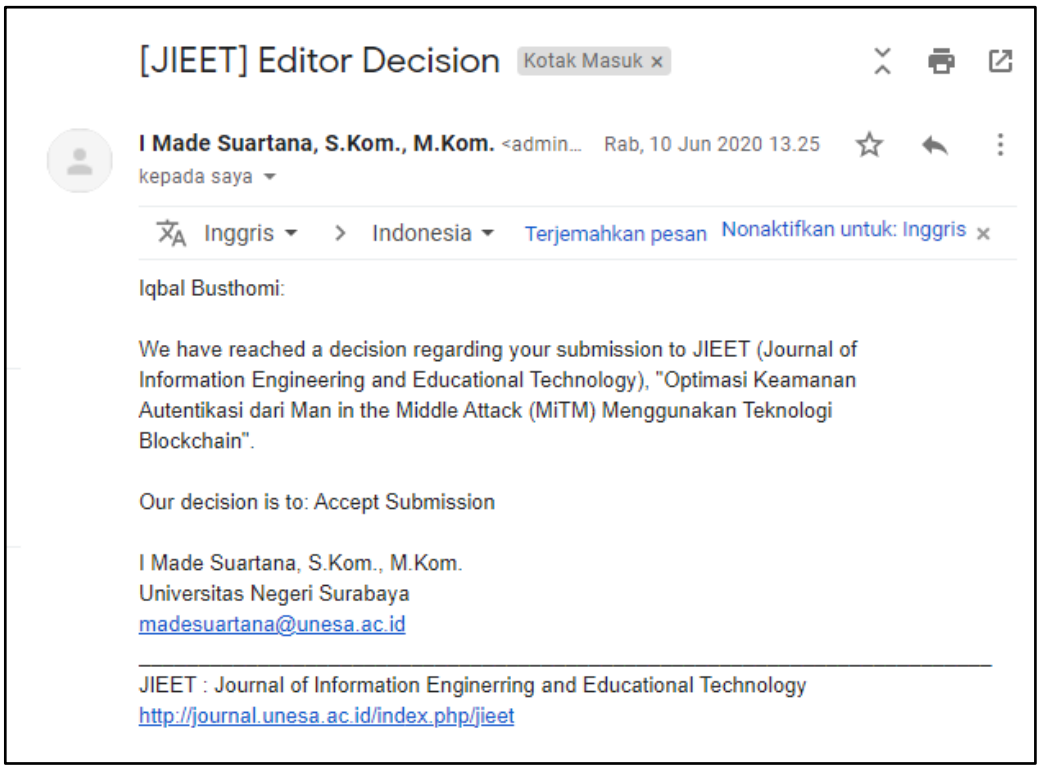
1. Prior to proceeding with the review process, the manuscript (.docx) should be formatted according to JESTEC Template (attached). Please use this link to read the Guidelines for Submission of Contributions http://jestec.taylors.edu.my/instructions.html. Also take note please that our citation style and format of the references are unique. We do not follow any standard citation styles. Attached find the instructions how to prepare the references in terms of the style and format. Kindly take note that we will not start the review process until the manuscript is correctly and completely formatted according to JESTEC template and there are no technical mistakes and/or missing part.
2. Our review is double-blind, so based on JESTEC Template (for Blind Review), any information related to your identity must be removed. This includes the acknowledgment, appreciation, etc., if any.
3. Please download the PPR excel file and provide complete information (Paper's Details worksheet only). You are not allowed to modify the form. Just fill it completely with correct information. The information should include the similarity index, supported by the similarity report, nomination of at least 4 potential reviewers who are not from JESTEC list of reviewers. Note that the qualification of these reviewers must be Ph.D. with adequate knowledge of the paper topic, etc.

Kindly complete your submission as soon as possible as your submission will be considered declined without notification after 7 days from the date of this email.

Please be reminded that upon the full acceptance of your paper, publication fee in amount of USD300 must be paid before the article is published in the journal website.

Regards and greetings

JESTEC Editor
http://jestec.taylors.edu.my



[JIEET] Editor Decision Kotak Masuk ×

I Made Suartana, S.Kom., M.Kom. <admin... Rab, 10 Jun 2020 13.25

kepada saya

Inggris > Indonesia Terjemahkan pesan Nonaktifkan untuk: Inggris ×

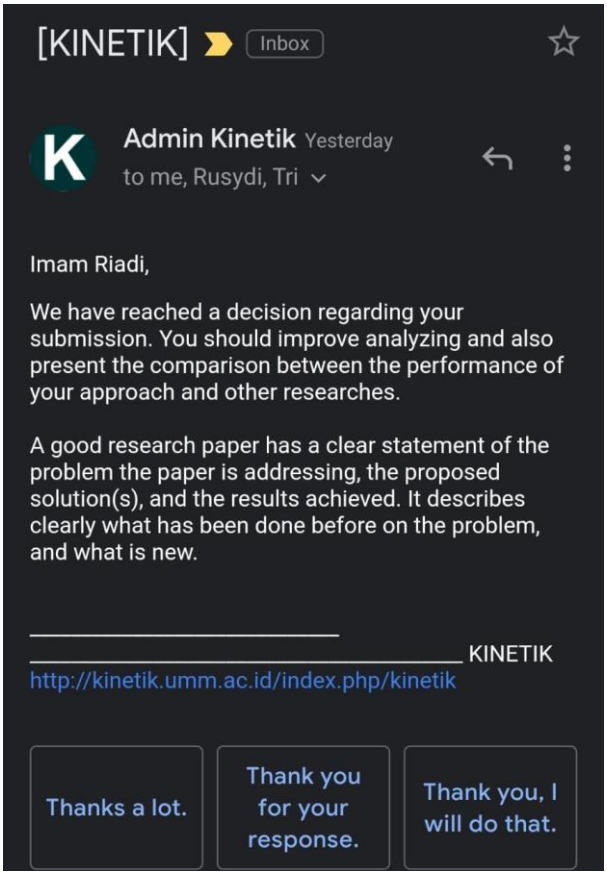
Iqbal Busthomi:

We have reached a decision regarding your submission to JIEET (Journal of Information Engineering and Educational Technology), "Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain".

Our decision is to: Accept Submission

I Made Suartana, S.Kom., M.Kom.
Universitas Negeri Surabaya
madesuartana@unesa.ac.id

JIEET : Journal of Information Enginerring and Educational Technology
http://journal.unesa.ac.id/index.php/jieet



[KINETIK] Inbox

Admin Kinetik Yesterday
to me, Rusydi, Tri

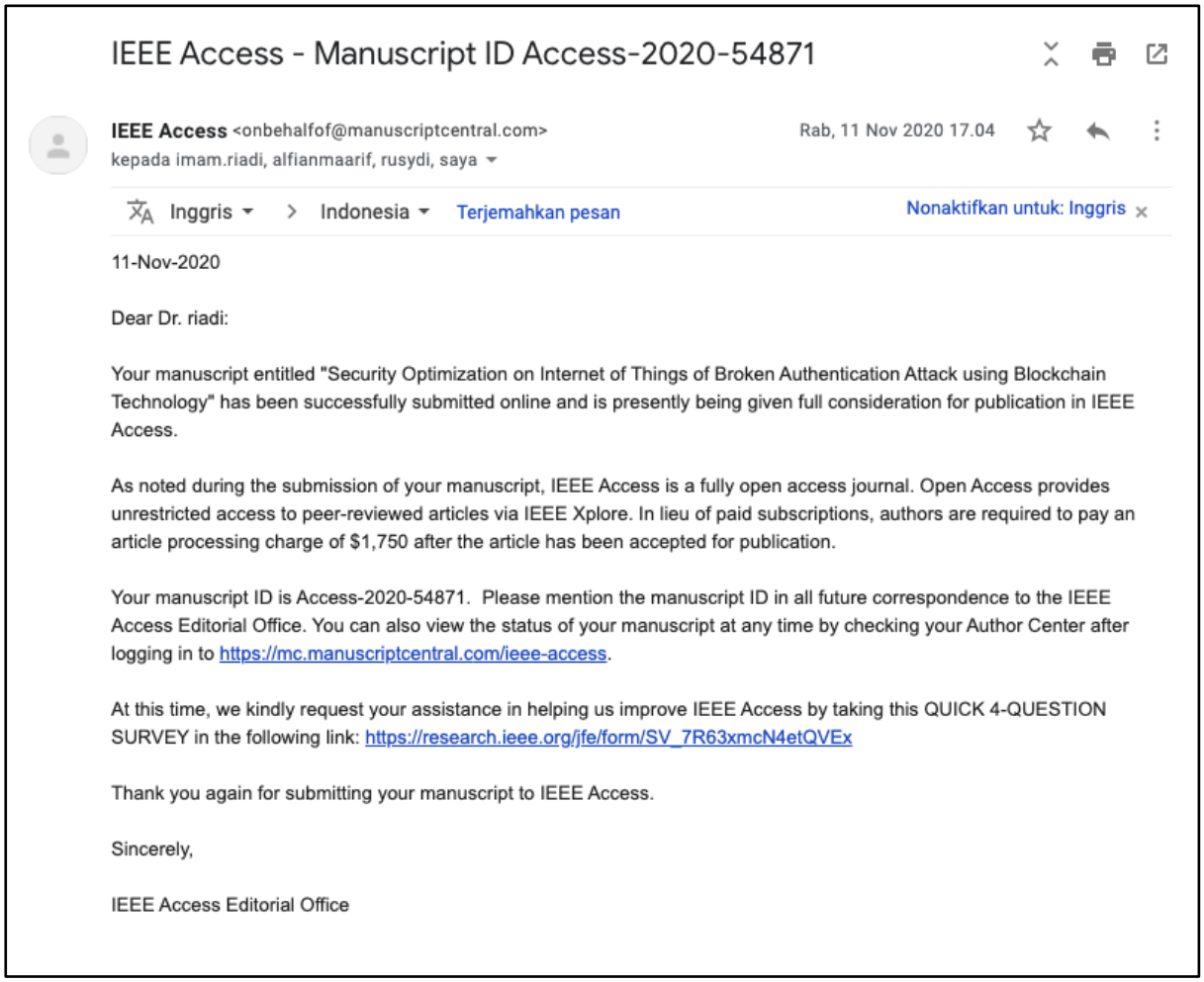
Imam Riadi,

We have reached a decision regarding your submission. You should improve analyzing and also present the comparison between the performance of your approach and other researches.

A good research paper has a clear statement of the problem the paper is addressing, the proposed solution(s), and the results achieved. It describes clearly what has been done before on the problem, and what is new.

KINETIK
http://kinetik.umm.ac.id/index.php/kinetik

Thanks a lot. | Thank you for your response. | Thank you, I will do that.



IEEE Access - Manuscript ID Access-2020-54871

IEEE Access <onbehalfof@manuscriptcentral.com> Rab, 11 Nov 2020 17.04
kepada imam.riadi, alfianmaarif, rusydi, saya

Inggris > Indonesia Terjemahkan pesan Nonaktifkan untuk: Inggris

11-Nov-2020

Dear Dr. riadi:

Your manuscript entitled "Security Optimization on Internet of Things of Broken Authentication Attack using Blockchain Technology" has been successfully submitted online and is presently being given full consideration for publication in IEEE Access.

As noted during the submission of your manuscript, IEEE Access is a fully open access journal. Open Access provides unrestricted access to peer-reviewed articles via IEEE Xplore. In lieu of paid subscriptions, authors are required to pay an article processing charge of $1,750 after the article has been accepted for publication.

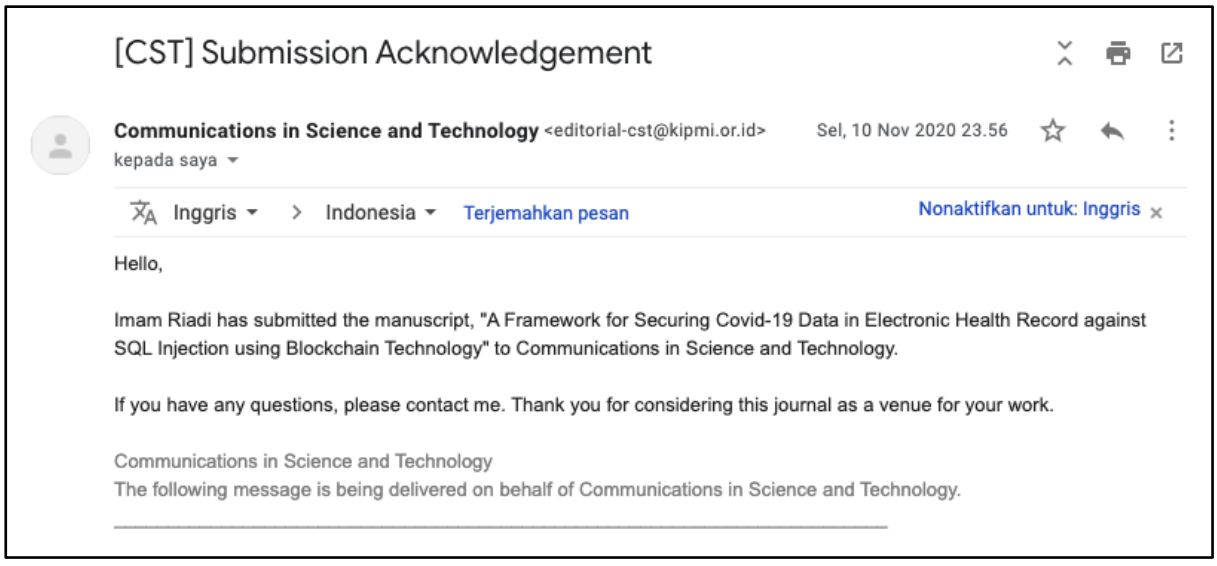
Your manuscript ID is Access-2020-54871. Please mention the manuscript ID in all future correspondence to the IEEE Access Editorial Office. You can also view the status of your manuscript at any time by checking your Author Center after logging in to https://mc.manuscriptcentral.com/ieee-access.

At this time, we kindly request your assistance in helping us improve IEEE Access by taking this QUICK 4-QUESTION SURVEY in the following link: https://research.ieee.org/jfe/form/SV_7R63xmcN4etQVEx

Thank you again for submitting your manuscript to IEEE Access.

Sincerely,

IEEE Access Editorial Office



[CST] Submission Acknowledgement

Communications in Science and Technology <editorial-cst@kipmi.or.id> Sel, 10 Nov 2020 23.56
kepada saya

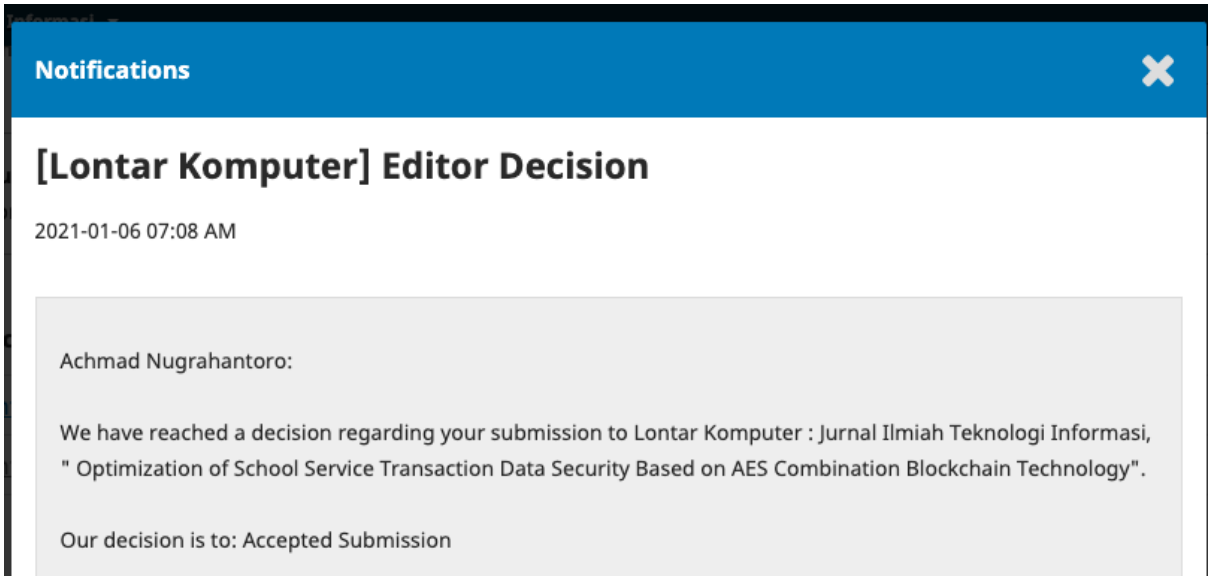
Inggris > Indonesia Terjemahkan pesan Nonaktifkan untuk: Inggris

Hello,

Imam Riadi has submitted the manuscript, "A Framework for Securing Covid-19 Data in Electronic Health Record against SQL Injection using Blockchain Technology" to Communications in Science and Technology.

If you have any questions, please contact me. Thank you for considering this journal as a venue for your work.

Communications in Science and Technology
The following message is being delivered on behalf of Communications in Science and Technology.



Notifications

[Lontar Komputer] Editor Decision

2021-01-06 07:08 AM

Achmad Nugrahantoro:

We have reached a decision regarding your submission to Lontar Komputer : Jurnal Ilmiah Teknologi Informasi, " Optimization of School Service Transaction Data Security Based on AES Combination Blockchain Technology".

Our decision is to: Accepted Submission

LAMPIRAN 7

(Jurnal Internasional dan Jurnal Nasional)

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Security Optimization on Internet of Things of Broken Authentication Attack using Blockchain Technology

Imam Riadi[1]*, Alfian Ma'arif[2], Member, IEEE, Rusydi Umar[3], Purwono[4]

[1]Department of Information System, Universitas Ahmad Dahlan, 55191, Indonesia
[2]Department of Electrical Engineering, Universitas Ahmad Dahlan, 55191, Indonesia
[3,4]Department of Informatics Engineering, Universitas Ahmad Dahlan, 55191, Indonesia

Corresponding author: Imam Riadi (e-mail: imam.riadi@is.uad.ac.id).

ABSTRACT The increased use of Internet of Things (IoT) technology must be balanced with the security of data transactions, especially in the cryptocurrency sector. The use of the REST API to send transaction data by IoT devices must consider security gaps to be safe from cyber-attacks. One of the most frequent attacks is the Broken Authentication by irresponsible parties for stealing user profile data. These data are usually misused for criminal purposes that can harm individuals or organizations; therefore, a solution is needed to improve the security of IoT data transactions. This paper provides a suggestion of a security optimization model with several levels of REST API security on the IoT, namely utilizing the application of JWT and Blockchain Technology. The test was done by performing 10 attacks to manipulate transaction data by attackers by making a fake keypair; the result showed that the data is safe. Another anticipation when keypair is successfully obtained is the validation of each chain with a consensus algorithm. Hence, the manipulated transaction data can be returned to the condition agreed by the blockchain network members.

INDEX TERMS Internet of Things (IoT), JSON Web Token, Broken Authentication, REST API, Blockchain.

I. INTRODUCTION

The popularity of the Internet of Thing (IoT) technology is increasing rapidly. IoT is one of the most influential technologies in Industry 4.0 [1]. IoT allows all things to be connected to the internet network based on predetermined protocols through information sensing equipment for information exchange and communication needs for specific purposes [2].

Data transmission in IoT technology can be done using the concept of web services [3]. Web service is a distributed computation in information technology that was developed after the discovery of website technology. Web services can compute on multiple machines and are also used by many machines [4]. One of the most popular web services is REST (Representational State Transfer) [5]. REST is an architectural design of a web service where the design has a source that can be accessed via a unique HTTP URL address. REST allows users to make requests via the HTTP protocol easily [6]. IoT utilizes the REST API (Application Programming Interface) to send data, which is commonly called the IoT API. API technology is a link between modern applications. Almost all applications use an API to connect with the corporate, third party, or other data sources [7].

Web services security is among the top ten vulnerabilities in the under-protected Web Services API security, according to The Open Web Application Security Project (OWASP) [4]. This is an important scourge related to the security of data transactions carried out by IoT. One of the most common attacks on Web Services is Broken Authentication. Weak system designs such as errors in authentication configurations and session management risk exploitation of vulnerabilities by attackers [8]. The attacker tries to take over important data, such as personal and important user profile information [9]. One of the important data is the login information in the form of a specific username and password to access other confidential data. System takeover can occur and not only data theft, even data destruction or data misuse by irresponsible people.

Overcoming security risks from Broken Authentication attacks on IoT applications, one of which can be layered security, namely the addition of JSON Web Token (JWT) to Blockchain technology authentication and modeling in the REST API design. Blockchain technology will be the final foundation when JWT can be stolen in the event of a Broken Authentication attack.

This paper presents an IOT data security optimization model from a Broken Authentication attack by combining the JWT concept and Blockchain Technology.

II. RELATED WORKS

Optimization of IoT security with Blockchain technology has been carried out by [10], produced an adaptive security framework for IoT architecture with Blockchain technology. The security framework consists of dynamic resource calculation algorithms based on networks that adapt to existing resources and decide which security services to offer.

Research conducted by [1] proposed data security modeling with Blockchain technology as an alternative solution to improve the security of management of various IoT data in three main criteria, including confidentiality, integrity, and availability.

Research conducted by [11] produced a lightweight architectural model for IoT security using the Ethereum Blockchain, which maintains most of its security. This model used the Blockchain decentralized concept, which solves a single authentication problem on the IoT network.

Research conducted by [12] carried out an IoT data security survey with Blockchain technology. The main focus that must be considered while securing data is the sensitivity of the scattered data in the IoT environment. Blockchain has great potential as an IoT security solution, especially in the financial sector.

III. PROPOSED METHODS

A new approach to optimizing the security of IOT APIs from Broken Authentication attacks is proposed by combining two levels of security, namely the application of JWT and Blockchain technology. The general flow of this security optimization can be seen in Figure 1.

Initially, IoT Devices send transaction data with the REST API service to the server. Transaction data is stored automatically with the ledger concept on all Blockchain members. Any information that will be sent enters the pending transaction data. After each member has done data mining, data will be entered in each block of each member. All data transaction transmission history will be stored properly on each member's computer. Transaction data access security is implemented at three layers: authentication using a login system, JWT application to Blockchain technology.

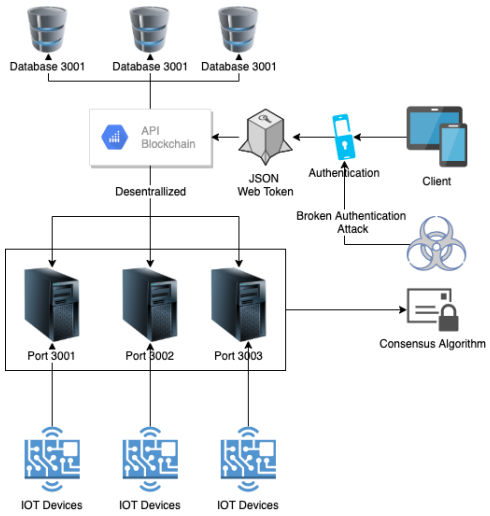


FIGURE 1. The general flow of IoT security optimization

Attackers will face the first security level, which is having to guess the username and password as an authentication tool to access the following data. Suppose the attacker can get the username and password data with Broken Authentication. In that case, the attacker must compete with the expiration time of a token that was created with JWT. If the attacker can manipulate the timing of the token, the attacker can access the API data. At this stage, the attacker will usually try to modify certain data. Changing data seemed successful initially, but Blockchain uses a decentralized concept that utilizes a consensus algorithm where all transactions will be equalized on each Blockchain network. Data manipulation efforts are then useless no matter how often it is done unless it has to attack all Blockchain members.

A. LOGIN AUTHENTICATION

Login is used to authenticate which users have the right to access confidential data. The authentication process is used to distinguish the characteristics of each user. Privileges are granted to users who already have certain access keys [13]. The most common authentication that we can see is that the user is confronted with a login page or URL. The user must enter a username and password as the secret page access key. Requested passwords are usually encrypted into a specific format.

B. JSON WEB TOKEN (JWT)

JWT is a JSON object defined in RFC 7519 as a secure way of representing a collection of information between two parties [14]. A token will be generated if the user successfully logs in by entering the appropriate username and password in the database. The token will be stored in browser cookies. The token is used to access certain pages. The user will send the token back in the authorization header as proof that the user has logged in.

Figure 3 [14] shows an example of using JWT. There are three main parts to JWT, namely:

- header, describes primitives in JSON format that are used to secure claims.
- payload, or entity, describing the claim in JSON format.
- signature or message authentication code in header64, which is encoded in header and payload

B. BLOCKCHAIN TECHNOLOGY

Blockchain technology is a system with the concept of recording public ledger transaction data. Blockchain is decentralized and distributed, which utilizes a consensus scheme that allows transaction data to be safely stored on the Blockchain network after going through the verification and validation process without any third-party intervention [15]. All transaction data will be recorded on all Blockchain networks, and of course, this is not centered on just one party. This technology will record all transactions at each node to make it difficult to modify by irresponsible people [16]. Figure 2 illustrates an example of Blockchain implementation. With the previous block's hash contained in the block header, a block has only one permanent block. The first block of the Blockchain is referred to as the genesis block, which has no parent block [17].

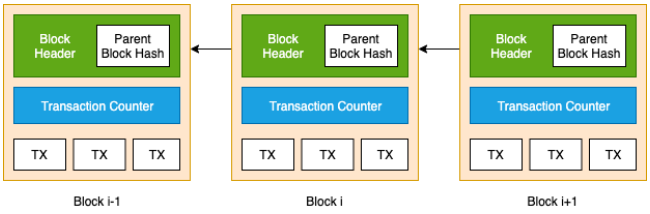


FIGURE 2. An example of a Blockchain consisting of continuous blocks

B. CONSENSUS ALGORITHM

A consensus algorithm is a protocol used to reach an agreement on a single data value. The consensus algorithm is mechanistic and automatically synchronizes all transaction data on the Blockchain [18]. This algorithm mechanism first requires ascertaining the state of the network and determining which nodes can validate transactions. One of the consensus algorithms available is proof-of-work (PoW), which requires solving complex math in cryptography through a node on the network. Hence, it can run along, and random processes are providing answers to basic experiments and errors. [19]. It can be easily concluded that this algorithm produces majority decisions in a group. All members must accept this majority decision. Members who disagree with the majority decision are considered no longer members. The actual implementation in aligning transaction data in the blockchain network is that when one of the transaction data is different from most network data, it is considered invalid. This makes for great security in protecting the data of all members.

IV. RESULTS AND DISCUSSION

This section shows the testing of the security optimization of the IoT API from a Broken Authentication attack. The first stage, the creation of IoT device functionality. The second stage is the creation of a member authentication process with a login and JWT system. The third stage is the creation of the IoT API synchronization series with the Blockchain network. The fourth stage is testing the security of sending transaction data.

A. IOT DEVICE

In this study, the IoT Device will be used as a demonstration of sending cryptocurrency transaction data. The device is set to send data automatically through sensors, namely data on the sender, receiver, and nominal cryptocurrency sent.

B. JWT TOKEN AUTHENTICATION AND GENERATE

Transaction data sent must pass the authentication stage. Members must first log in by entering their username and password. The creation of a JWT token indicates successful authentication. Figure 3 is an example of making a JWT token if the user has successfully entered the correct username and password data.


```
"id": "5f510106df45e9556612585c",
"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
    eyJzdWIiOiI1ZjUxMDEwNmRmNDVlOTU1NjYxMjU4NWMiLCJpYXQiOjE1OTkyMDA4NjUsImV4cCI6MTU5OTgwNTY2NX0.
    Qul78HxC6yhPJ6LAKscAR_Yb2ma9Ifi8UTURwnw9R7I"
```


FIGURE 3. JWT Token after Login

C. BLOCKCHAIN TECHNOLOGY

The making of Blockchain technology features will be synchronized with all transactions made by the IoT device. Each member on the Blockchain decentralized network has a private key pair [20]. Transactions without key pairs cannot be carried out. Members connected to the Blockchain network are not allowed to make changes or delete block transactions [21]. Transactions are also safe from third party interference [22]. The chain which contains blocks connected to each other will continue to be the consensus so that blocks containing invalid transaction values can be ignored by other users or deleted on the network automatically. A consensus is needed to ensure that Blockchain is running properly [23]. Figure 4 is the code to confirm whether a member has a key pair or not.

```
signTransaction(signingKey) {
  if (signingKey.getPublic('hex') !== this.fromAddress) {
    throw new Error('You cannot sign transactions for other wallets!');
  }
  const hashTx = this.calculateHash();
  const sig = signingKey.sign(hashTx, 'base64');
  this.signature = sig.toDER('hex');
}
```

FIGURE 4. Sign Transaction Key

The application of the consensus algorithm (proof of work) can be seen in Figure 5.

```
mineBlock(difficulty) {
  while (this.hash.substring(0, difficulty) !== Array(difficulty + 1).join('0')) {
    this.nonce++;
    this.hash = this.calculateHash();
  }

  debug(`Block mined: ${this.hash}`);
}
```

FIGURE 5. Proof of Work

The proof of work process can also be called the mining process. Modern computers can make transactions quickly; we can provide difficulties in solving hash blocks [24]. The purpose of this proof of work is to avoid invalid chains or attempts by miners to commit fraudulent transactions. Invalid chains will then be ignored or deleted by the Blockchain network; therefore, we need a nonce, a random integer number used as the identity for the next hash generation.

D. SECURITY TESTING OF BROKEN AUTHENTICATION ATTACKS

One of the IoT API security tests can be done using the Burp Suite application [25]. This application can be used to detect an application's weakness, one of which is the authentication vulnerability that is easy to guess. User authentication obtained with the Broken Authentication attack is then used for logging in and manipulating transaction data.

An attacker who has successfully logged in cannot immediately make changes to the data because every transaction requires a keypair. The nature of each keypair that is owned by the Blockchain network member is private, so the attacker must create a keypair that is similar to what the member has. Table 1 is an attempt by attackers to attempt to manipulate transaction data. This attack simulation is carried out 10 times with the keypair test that the attacker has made. Table 1. Trial of making transaction blocks with keypair

TABLE I
TRIAL OF MAKING TRANSACTION BLOCKS WITH FAKE KEYPAIR

Testing	Fake Keypair	Result
1	8574737317a611884592d0761bb71e6da5635f85192f0323843d596003e49fe01	"Cannot read property 'privateKey' of null"
2	525262526a611884592d0761bb71e6da5635f85192f0323843d596003e49fe019	"Cannot read property 'privateKey' of null"
3	95858575a611884592d0761bb71e6da5635f85192f0323843d596003e49fe019r	"Cannot read property 'privateKey' of null"
4	415225252a611884592d0761bb71e6da5635f85192f0323843d596003e49fe017	"Cannot read property 'privateKey' of null"
5	969686865a611884592d0761bb71e6da5635f85192f0323843d596003e49fe018	"Cannot read property 'privateKey' of null"
6	9685747474a611884592d0761bb71e6da5635f85192f0323843d596003e49fe01j	"Cannot read property 'privateKey' of null"
7	5252262626a611884592d0761bb71e6da5635f85192f0323843d596003e49fe019	"Cannot read property 'privateKey' of null"
8	736363535a611884592d0761bb71e6da5635f85192f0323843d596003e49fe01jk	"Cannot read property 'privateKey' of null"
9	413132526a611884592d0761bb71e6da5635f85192f0323843d596003e49fe01yy	"Cannot read property 'privateKey' of null"
10	958575777a611884592d0761bb71e6da5635f85192f0323843d596003e49fe015t	"Cannot read property 'privateKey' of null"

Ten tests can be seen in Table 1. The fake keypair cannot be used to manipulate transaction data, so the transaction data is still considered safe. Anticipating conditions where hackers can find the same keypair code composition as members, Blockchain technology will validate each connected chain. Table 2 compares attempts to change the value of the transaction block by hackers and validate it with a validation code. Figure 6 is the code for validating the transaction block.

```
isChainValid() {
  const realGenesis = JSON.stringify(this.createGenesisBlock());
  if (realGenesis !== JSON.stringify(this.chain[0])) {
    return false;
  }
  for (let i = 1; i < this.chain.length; i++) {
    const currentBlock = this.chain[i];
    if (!currentBlock.hasValidTransactions()) {
      return false;
    }
    if (currentBlock.hash !== currentBlock.calculateHash()) {
      return false;
    }
  }
  return true;
}
```

FIGURE 6. Transaction block validation

TABLE II
ATTEMPTS TO CHANGE TRANSACTION BLOCK DATA

Parameter	Blok
Original	Id: 5f51efb2eea5600c7d1e9b02 Timestamp: 2020-09-04T07:41:38.275Z Transaction: [fromAddress:ipung, toAddress:iqbal amount: 60,signature: 3044022018cd20e21dad79417453892035 8b7926288003493] previousHash: 0 nonce: 19 hash: **008594849 7a97c5022154876 44df8b8579331b38ec8aacc505f230debc7c8810**
	Id: 5f51efb2eea5600c7d1e9b02 Timestamp: 2020-09-04T07:42:02.116Z Transaction: [fromAddress:ipung, toAddress:johan amount: 30,signature: 3046022100f663547efaee2b6e4074e442b7fdd3b75c2911a4f] previousHash: **008594849 7a97c5022154876 44df8b8579331b38ec8aacc505f230debc7c8810** nonce: 53 hash: **00afa96c23a16c0af2dfbccd9a102ef73ba69b2031e65552d50b24349db34438**

	Id: 5f51efb2eea5600c7d1e9b02 Timestamp: 2020-09-04T07:44:41.978Z Transaction: [fromAddress:ipung, toAddress:tari amount: 50,signature: 04a642c9403b8bf52d5e8246ee3165effe94670b359d508e22] previousHash: **00afa96c23a16c0af2dfbccd9a102ef73ba69b2031e65552d50b24349db34438** nonce: 41 hash: 0009872fee555d5735546d2a0056a087fbf141584ee45620756ced49359366ba **Status: Valid**
Block Changed	Id: 5f51efb2eea5600c7d1e9b02 Timestamp: 2020-09-04T07:41:38.275Z Transaction: [fromAddress:ipung, toAddress:iqbal amount: 60,signature: 3044022018cd20e21dad7941745389203 58b792628800 3493] previousHash: 0 nonce: 19 hash: **0085948497a97c502215487644df8b8579331b38ec8aacc505f230debc7c8810**
	Id: 5f51efb2eea5600c7d1e9b02 Timestamp: **2020-09-04T10:06:42.394Z** Transaction: [fromAddress:ipung, toAddress:johan **amount: 100**,signature: **3045022100a13207a3434c136fe39e966097dc9640c54b2b7449**] previousHash: **0085948497a97c502215487644df8b8579331b38ec8aacc505f230debc7c8810** nonce: 53 hash: **000c93c8b7440bbd5903f8adc62f8bf393d40a07f9e618de6ad3511a335fd5ff**
	Id: 5f51efb2eea5600c7d1e9b02 Timestamp: 2020-09-04T07:44:41.978Z Transaction: [fromAddress:ipung, toAddress:tari amount: 50,signature: 04a642c9403b8bf52d5e8246ee3165effe94670b359d508e22] previousHash: **00afa96c23a16c0af2dfbccd9a102ef73ba69b2031e65552d50b24349db34438** nonce: 41 hash: 0009872fee555d5735546d2a0056a087fbf141584ee45620756ced49359366ba **Status: Invalid**
Block After Proof of Work	Id: 5f51efb2eea5600c7d1e9b02 Timestamp: 2020-09-04T07:41:38.275Z Transaction: [fromAddress:ipung, toAddress:iqbal amount: 60,signature: 3044022018cd20e21dad7941745389203 58b792628800 3493] previousHash: 0 nonce: 19 hash: **0085948497a97c502215487644df8b8579331b38ec8aacc505f230debc7c8810**
	Id: 5f51efb2eea5600c7d1e9b02 Timestamp: 2020-09-04T07:42:02.116Z Transaction: [fromAddress:ipung, toAddress:johan amount: 30,signature: 3046022100f663547efaee2b6e4074e442b7fdd3b75c2911a4f] previousHash: **0085948497a97c502215487644df8b8579331b38ec8aacc505f230debc7c8810** nonce: 53 hash: **00afa96c23a16c0af2dfbccd9a102ef73ba69b2031e65552d50b24349db34438**
	Id: 5f51efb2eea5600c7d1e9b02 Timestamp: 2020-09-04T07:44:41.978Z Transaction: [fromAddress:ipung, toAddress:tari amount: 50,signature: 04a642c9403b8bf52d5e8246ee3165effe94670b359d508e22] previousHash: **00afa96c23a16c0af2dfbccd9a102ef73ba69b2031e65552d50b24349db34438** nonce: 41 hash: 0009872fee555d5735546d2a0056a087fbf141584ee45620756ced49359366ba **Status: Valid**

The proof of work method can be used to validate the value of each connected block. Blocks with a different transaction value from the majority in a Blockchain network will be eliminated, and the value stored in each blockchain member data will be corrected.

VII. CONCLUSION

Security in cryptocurrency transactions using IoT devices needs to be considered. Transaction data security threats such as changes in value can occur with various attacks, one of which is Broken Authentication, which can take user access rights. Taking access rights allows a change of control in transactions that could potentially harm the user. User authentication, which is generally secured using a login and JWT access, is possible to be attacked; therefore, we need to increase the security layer. Blockchain technology is used as one of the models used in this research. Blockchain with private keypair and proof of work methods can validate the security of transaction data. The experiment used 10 attempts to manipulate transaction data by hackers with fake keypair, resulting in failing to manipulate transaction data. Validation is also used to keep the submitted data consistent and integrated. Hackers can take over user access rights with Broken Authentication. However, hackers are unable to make attempts to change transaction data due to data decentralization on the Blockchain network. We are still working to do further research to produce more precise data accuracy. The resulting data may still be imperfect; we can do more testing and use other attack tools to prove that Blockchain technology is a good method to secure transaction data.

REFERENCES

[1] H. A. Pham, T. K. Le, T. N. M. Pham, H. Q. T. Nguyen, and T. Van Le, "Enhanced Security of IoT Data Sharing Management by Smart Contracts and Blockchain," Proceedings - 2019 19th International Symposium on Communications and Information Technologies, ISCIT 2019, no. September, pp. 398–403, 2019.

[2] K. K. Patel and S. M. Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges," International Journal of Engineering Science and Computing, vol. 6, no. 5, pp. 1–10, 2016.

[3] M. Thiyagarajan and C. Raveendra, "Role of web service in Internet of Things," Proceedings of the 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology, iCATccT 2017, pp. 268–270, 2018.

[4] A. Rahmatulloh, H. Sulastri, and R. Nugroho, "RESTful Web Service Security Using JSON Web Token (JWT) HMAC SHA-512," Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI), vol. 7, no. 2, 2018.

[5] A. Soni and V. Ranga, "API features individualizing of web services: REST and SOAP," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue, pp. 664–671, 2019.

[6] M. I. Perkasa and E. B. Setiawan, "Community Data Web Service Development Using REST API with Access Token," Jurnal ULTIMA Computing, vol. 10, no. 1, pp. 19–26, 2018.

[7] B. Di Martino, A. Esposito, S. A. Maisto, and S. Nacchia, "A semantic IoT framework to support RESTful devices' API interoperability," Proceedings of the 2017 IEEE 14th International Conference on Networking, Sensing and Control, ICNSC 2017, no. May, pp. 78–83, 2017.

[8] M. M. Hassan et al., "Broken Authentication and Session Management Vulnerability: A Case Study of Web Application," International journal of simulation: systems, science & technology, pp. 1–11, 2018.

[9] M. F. Haque, M. B. A. Miah, and F. Al Masud, "Enhancement of Web Security Against External Attack," European Scientific Journal, ESJ, vol. 13, no. 15, p. 228, 2017.

[10] V. Mathane and P. V. Lakshmi, "Adaptive security framework for the blockchain on IoT," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9, pp. 3327–3331, 2019.

[11] P. Ghadekar, N. Doke, S. Kaneri, and V. Jha, "Secure access control to IoT devices using blockchain," International Journal of Recent Technology and Engineering, vol. 8, no. 2, pp. 3064–3070, 2019.

[12] E. F. Jesus, V. R. L. Chicarino, C. V. N. De Albuquerque, and A. A. D. A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," Security and Communication Networks, vol. 2018, 2018.

[13] Y. Balaj, "Token-Based vs Session-Based Authentication : A survey," no. September, pp. 1–6, 2017.

[14] K. Shingala, "JSON Web Token (JWT) based client authentication in Message Queuing Telemetry Transport (MQTT)," no. March, 2019.

[15] S. S. Sarmah, "Understanding Blockchain Technology," Computer Science and Engineering, vol. 8, no. 2, pp. 23–29, 2018.

[16] 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 International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019, no. July, pp. 1–7, 2019.

[17] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, no. June, pp. 557–564, 2017.

[18] R. P. dos Santos, "Consensus Algorithms: A Matter of Complexity?," in Blockchain Economics : Implication of Distributed Ledgers, no. June, 2019, pp. 147–170.

[19] B. Lucas and R. V. Paez, "Consensus algorithm for a private blockchain," ICEIEC 2019 - Proceedings of 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication, no. July, pp. 264–271, 2019.

[20] M. Aydar, S. C. Cetin, S. Ayvaz, and B. Aygun, "Private key encryption and recovery in blockchain," no. July, pp. 0–22, 2019.

[21] P. Tasca and C. J. Tessone, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification," Ledger, vol. 4, pp. 1–39, 2019.

[22] R. Stephen and A. Alex, "A Review on BlockChain Security," IOP Conference Series: Materials Science and Engineering, vol. 396, no. 1, 2018.

[23] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," ICOSST 2018 - 2018 International Conference on Open Source Systems and Technologies, Proceedings, no. May 2020, pp. 54–63, 2019.

[24] A. A. G. Agung, R. G. Dillak, D. R. Suchendra, and H. Robbi, "Proof of work: Energy inefficiency and profitability," Journal of Theoretical and Applied Information Technology, vol. 97, no. 5, pp. 1623–1633, 2019.

[25] H. Saputera, "Software Security Testing on Broken Authentication and Security Misconfiguration Factors," Universita Islam Indonesia, 2018.

IMAM RIADI received a bachelor's degree in the Department of Electrical Engineering Education, Universitas Negeri Yogyakarta, Indonesia in 2001. He received the master's degree in Department of Computer Science, Universitas Gadjah Mada, Indonesia in 2003. He received the doctor's degree in Department of Computer Science, Universitas Gadjah Mada, Indonesia in 2014.

Currently, he was a lecturer in the Department of Information System, Universitas Ahmad Dahlan. His research interest includes Information Security, Computer Network, Network Security, Digital Forensics, Network Cloud Forensics

ALFIAN MA'ARIF (M'20) received a bachelor's degree in the Department of Electrical Engineering, Universitas Islam Indonesia, Indonesia in 2014. He received the Master of Engineering in Department of Electrical Engineering, Universitas Gadjah Mada, Indonesia in 2017.

From 2019 until now, he was a lecturer in the Department of Electrical Engineering, Universitas Ahmad Dahlan. His research interest includes control system and computer programming.

RUSYDI UMAR received a bachelor's degree in the Department of Electrical Engineering, Universitas Gadjah Mada, Indonesia in 1998. He received the master's degree in Department of Informatics Engineering, Institut Teknologi Bandung in 2003. He received the doctor's degree in School of Computer and Information Sciences, Hyderabad Central University, Hyderabad, India 2014.

Curently, he was a lecturer in Department of Informatics Engineering in, Universitas Ahmad Dahlan. His research interest includes Blockchain, Data mining, Cloud Computing and Digital Forensics

Purwono received a bachelor's degree in the Department of Information Systems, STIKOM Yos Sudarso Purwokerto, Indonesia in 2019. He received the master's degree in Department of Informatics Engineering, Universitas Ahmad Dahlan, Indonesia in 2020.

His research interest includes Machine Learning, Blockchain, Mobile Technology, Data Mining and Internet of Things.

p-ISSN: XXXX-YYYY
e-ISSN: XXXX-YYYY

Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology Modification

Abdul Fadlil[1], Imam Riadi[2], Achmad Nugrahantoro[3]

[1]Department of Electrical Engineering, Ahmad Dahlan University
[2]Department of Information Systems, Ahmad Dahlan University
[3]Department of Informatics Engineering, Ahmad Dahlan University
Jl. Prof. Dr. Soepomo, S.H, Janturan, Warungboto, Umbulharjo, Yogyakarta, Indonesia
[1]fadlil@mti.uad.ac.id
[2]imam.riadi@is.uad.ac.id
[3]achmad1907048001@webmail.uad.ac.id (Corresponding author)

Abstract

The application of Blockchain technology has begun to be widely accommodated in industrial and business practitioner environments as a safeguard of transaction security so that now including the education sector as non-business institutions enjoy the use of this technology to support the learning process. Information on the protected Blockchain can be in the form of transactions, assets, identities, and other information packaged in digital form. Information is collected in the form of blocks that are interrelated by using the hash function as cryptographic encryption. This research uses Blockchain for online pocket money top-up transactions for students. The use of a centralized Blockchain is centralized to reduce server procurement costs, but to increase the security of transaction information, modification of each block series is carried out using the AES cryptographic approach. The results showed that the attack by inserting a Cross-Site Scripting (XSS) script if you want to know the value of the top-up transaction amount, you must be able to hack the cryptographic process. This is supported by chain validation testing to determine how many block changes have been changed.

Keywords: *Blockchain, Cryptography, AES, Transaction, Education*

1. Introduction

Blockchain is a technology that involves third parties in the process of exchanging information. Information on the Blockchain can be in the form of data entry in the form of transactions, assets, identities, and other information that is packaged in digital form [1]. The form of blockchain information is easy to find, tends to be transparent and permanent, allowing users to monitor the history of information that occurs [2][3]. Blockchain technology is an alternative with a centralized technology architecture to support the disruption era. Conceptually, Blockchain is a technology with a distributed database that is stored and then shared with authorized users [3][4]. This concept is to replace the role of third parties such as financial institutions or other institutions, but on the literal side Blockchain technology is considered as a collection of interrelated blocks of information by utilizing the hash function as encryption in the field of cryptography [5][6].

Cryptography has become a science that has been widely used to maintain information security with mathematical calculation techniques [7][8]. This technique can convert plaintext using keys into random messages or ciphertext. There are several algorithms for data security, one of which is the Advanced Encryption Standard (AES) which is known as the standard crypto algorithm Data Encryption Standard (DES) [9][10]. AES is known to be resistant to differential attacks, namely conventional cryptographic cracking.

Technology with the use of Blockchain is not a new technology, that is, by involving old combinations with renewable means. For example, the relationship involves involving 3 (three) technologies, namely the internet, cryptography, and protocols from software, to produce strong security but still be able to interact or transact digitally. The relationship between Blockchain technology and cryptography is to position the role of cryptography with keys as an authentication

p-ISSN: XXXX-YYYY
e-ISSN: XXXX-YYYY

tool in terms of ownership of an authorized person. So that maintaining the confidentiality and content of the transaction prevents hacking. Besides, the cryptographic process is required to maintain the validity of broadcasting the contents of transaction information correctly, reducing failure and the risk of fraud to remain on the Blockchain protocol path.

The application of Blockchain technology has begun to be widely accommodated in industrial and business practitioners' environments as a safeguard of transaction security so that now including the education sector as non-business institutions enjoy the use of this technology to support the learning process. In the school system in Indonesia, there are several learning contracts for students that are required to pay for school needs such as school fees that are billed periodically every month, an obligation to save, and other transactions. Financial transactions are charged to students as the support for the sustainability of the school so that it requires the use of the internet in its digital interactions. The importance of recording risky financial transactions with costly data theft needs to present Blockchain technology as a solution. Not only that, Blockchain can reduce the involvement of many parties in online transactions because it allows building your network thus reducing costs both administratively and operationally.

Research with Blockchain in an educational environment is used to protect many useful assets such as digital document management such as in Nugraha's research [11], however, the research to be carried out involves financial transactions that occur in the school environment, namely with the online top-up pocket case studies. Putra's research combines Blockchain with RSA cryptography for data security on the network, the use of the RSA method affects the number of keys and its implementation cannot be directly applied to several devices [12]. In this research it is implemented on mobile android and Blockchain technology will be applied with AES which does not affect the size of the key. In the world of education, Blockchain technology is usually in the form of block certificates, book copyrights, and e-portfolios to avoid file forgery [13], as in Winarno's research using it for case studies of e-transcript publishing. Each application of Blockchain technology makes the attacker has to challenge the system for the formation of a longer blockchain, including for e- transcript cases. So this study will modify each series of blocks by utilizing the AES cryptographic approach to better maintain the integrity of stored messages, but applied to financial transactions that occur in the school environment. Another study conducted by Perdani [14] states that if financial technology needs to be protected from cybercrime, users still have easy access to financial transactions by increasing financial literacy. If FinTech involves many servers, it requires vendor consolidation and requires a high level of system security, then the proposed research will implement a centralized blockchain and efforts to increase its security with cryptographic techniques for each block of transactions.

Research by Benchoufi [15] has explored the core function of Blockchain as applied to clinical trials and the context of approval for trial protocols, the results of this study can help to check the integrity of clinical trials transparently but if a core metadata set is defined. The proposed research will be directed to use structured metadata, namely transaction data that occurs in the school environment, namely cases of online pocket money top-up transactions that are entered as student savings data. Other studies have summarized the use of Blockchain technology in several cases, namely for cryptocurrencies, smart contracts, smart cities, and this research proves that Blockchain technology has penetrated all areas of life [16]. So the research focuses on the educational environment in schools and implements case studies of financial transactions.

Blockchain in the research of Wright and Filippi [17] proves that if this approach makes it easy for users to access an automatic transaction system and an innovative governance model based on transparency, then this research will design its implementation until the assault testing scenario and validation results are planned. Blockchain-based platforms provide solutions for distributed data governance and participatory access control in the health sector which aims to improve Information Technology in the health sector [18], the health sector which aims to improve Information Technology in the health sector [18], Shabani's research is not yet in the implementation stage. So that researchers will implement it in the field of education. Another study in the health sector revealed that Blockchain is good at structuring data types in a decentralized manner which facilitates more transparent interactions [15]. However, the use of decentralization will cost money to procure a lot of servers. The research conducted utilizes centralization with a centralized server for financial transactions to be recorded in a transparent, centralized manner and can save costs.

The proposed method in the research uses a modified Advanced Encryption Standard (AES) cryptographic combination Blockchain technology for the protection of digital pocket money to up

p-ISSN: XXXX-YYYY
e-ISSN: XXXX-YYYY

transactions in a school environment. The workings of AES are in each blockchain resulting in higher security. The use of data in research uses structured data, namely, top-up transactions carried out by students, of course, this makes it easier to centralize a centralized server so that it remains recorded transparently and of course saves costs. To find out the resistance of the proposed algorithm modification, the test was carried out using the attack scenario with Cross-Site Scripting (XSS) and Chain Validation.

2. Research Methods

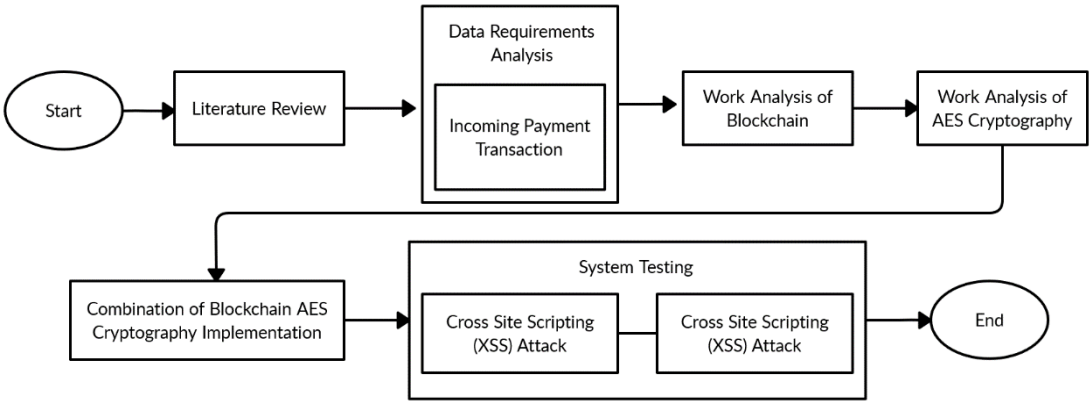


Figure 1. AES Combined Blockchain Technology Research Flowchart

The research uses Blockchain technology with AES cryptography to be utilized in the school environment, especially in pocket money top-up transactions as shown in Figure 1. Architectural analysis of Blockchain and Cryptography with the AES method, then how the two works are combined in securing transactions. The test scenario will be carried out by injection attack with Cross-Site Scripting (XSS) and test the validity of each block with Chain Validation.

2.1. Literature Review

The literature review by studying various sources in the form of descriptions of theory and findings obtained from books, similar research journals, scientific works, and other relevant sources. Especially the discussion regarding Blockchain technology and the performance of the AES cryptographic method.

2.2. Data Requirements Analysis

Researchers used a case study of top-up pocket money transactions in educational settings, especially schools. Pocket money top-up is a digital transaction made by students as savings which later can be useful for paying school needs such as bills, cash withdrawals, as infaq, zakat, and other transactions. The transactions that will be used and secured for the validity of the transactions are illustrated in Table 1 with the following data:

Table 1. Student Pocket Money Transaction Data

No.	ID Students	Name	Transaction	Amount	Information	Transaction Date
1.	4323	Namira Laura	Income	Rp. 3.000.000	Top Up	2020-05-23 13:03:45
2.	4112	Dwi Damayanti	Income	Rp. 250.000	Top Up	2020-05-30 13:03:45
3.	4321	Andri Reynaldi	Spending	Rp. 300.00	School costs and fees	2020-05-31 04:39:07
4.	4500	Titik Kirana Dewi	Income	Rp. 2.800.000	Top Up	2020-06-03 07:00:04
5.	4901	Habibah Rani Kireina	Spending	Rp. 300.000	School fees uniform	2020-06-04 19:42:21

In Table 1. the student pocket money transaction data consists of the student's identity number, full name, transactions that occur at that time according to the number of rupiah numbers, information about the transaction, and recording the transaction time. These data are protected,

p-ISSN: XXXX-YYYY
e-ISSN: XXXX-YYYY

especially in the data amount of the rupiah value top-up, the Blockchain process is carried out, and the AES cryptographic modification.

2.3. Blockchain Technology Architecture

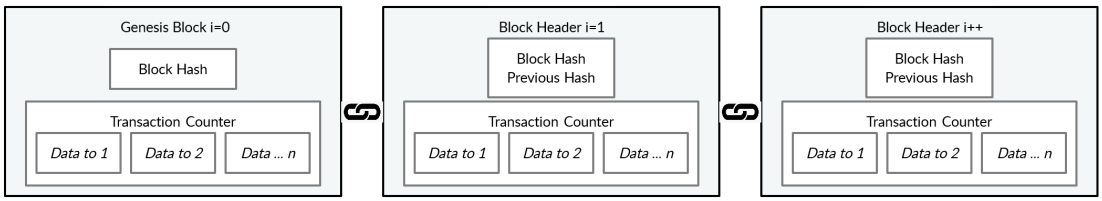


Figure 2. Blockchain Architecture Continous Sequence of Blocks

Figure 2. becomes an illustration of Blockchain architecture with a collection of transactions that occur and their history such as conventional ledger recording [19][20]. The description is a series of blockchain architectures with one block genesis at the beginning of block formation, then followed by a block header that is strung according to the previous hash. The Genesis Block is the first block in a series of blocks.

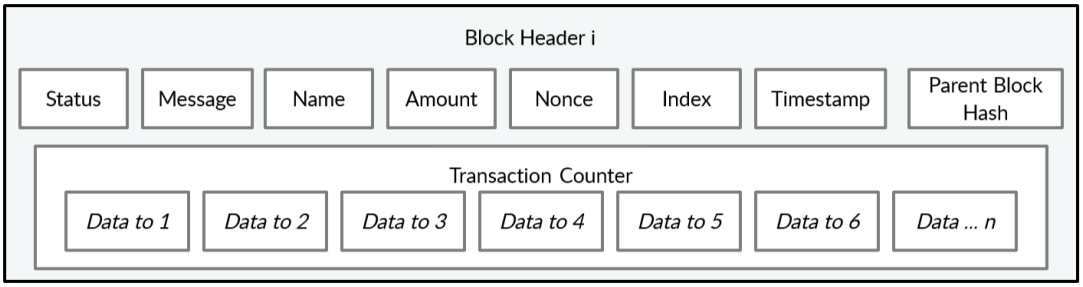


Figure 3. Single Block Structure

In Figure 3, it is explained that the contents of the block are the headers and contents of the blocks contained in online transactions on the school system that occur, namely an explanation of the transaction identity in status, message, name. In the entry, the amount is the number of transactions made in rupiah. The nonce is a 4-byte field that starts at 0 and will increase as the hash value is calculated. The index becomes the data described in each block and the timestamp becomes the universal time in the calculation of seconds. Parents Block Hash a 256-bit hash value that points to the previous block.

2.4. Advanced Encryption Standard (AES) Cryptographic Performance Analysis

Advanced Encryption Standard (AES) is one of the modern cryptographic methods as a replacement for the 56-bit block Data Encryption Standard (DES) algorithm which is considered unsafe [21][22]. The selection criteria of this algorithm are based on the characteristics, safety, and cost if used and their implementation. This algorithm is a single key by using the same key [10][23].

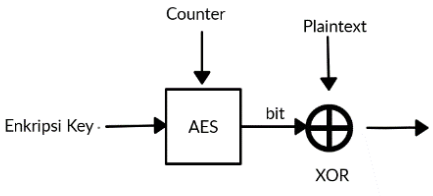


Figure 4. Single Key Cryptography AES

The description in FIgure 4. The encryption key is carried out by the AES process by previously receiving information, then processed with the selected bits. AES has assigned the bit lengths of the known keys AES-128, AES-192, and AES-256. Bit selection affects the key length, block size, and the number of rounds [24]. Plaintext or messages that will be processed in the cryptography process are XORed so that they produce meaningless messages. This study uses a 256-bit cryptographic key, with a key length of 8, block size 4, and the number of turns 14.

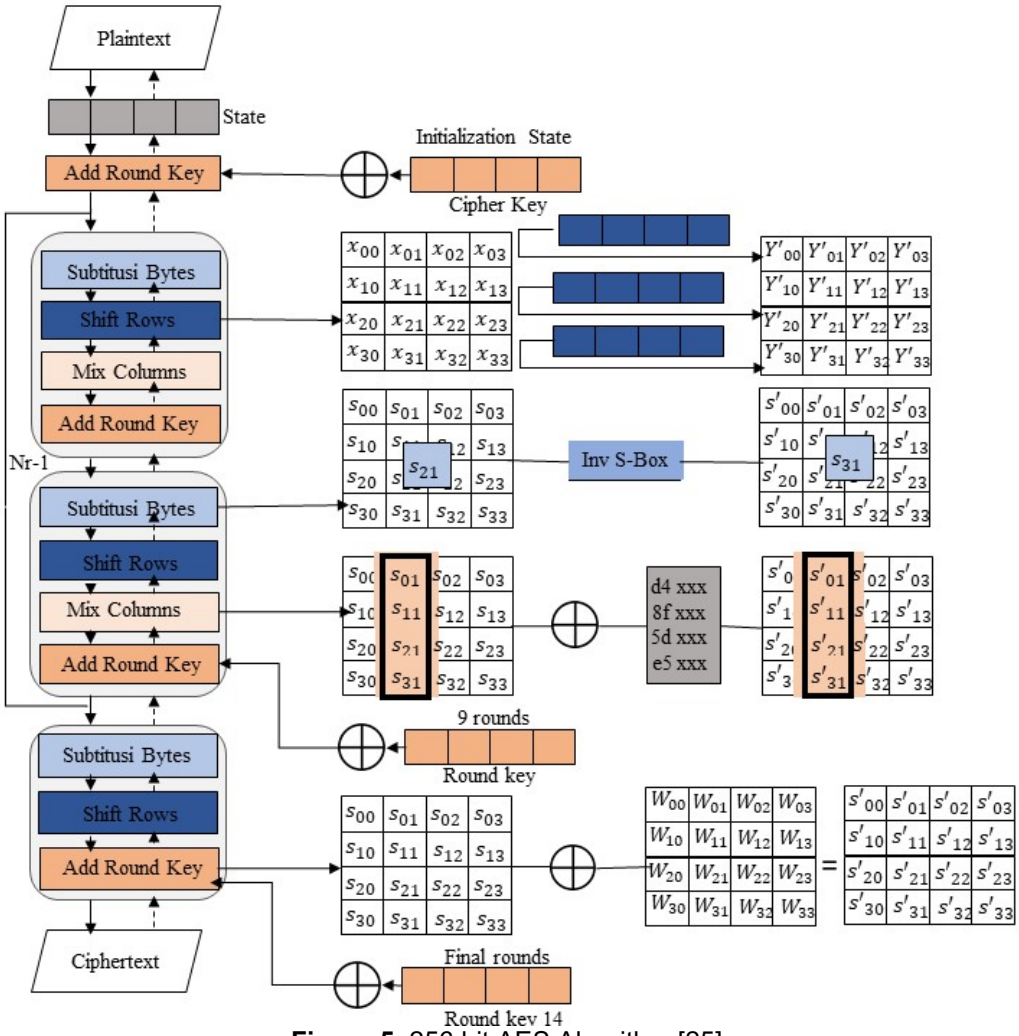


Figure 5. 256 bit AES Algorithm [25]

Figure 5 . is an outline of the AES algorithm that operates at 256 bits with the following information:

a. Add Round Key is this stage to be an initial round, namely initializing the initial state by XOR the plaintext process with a ciphertext key.
b. Round of Nr-*1* times, with 256 bits, then as many as Nr-14. Where in the process of each round includes the SubBytes process by substituting bytes with S-boxes, ShiftRows shifting on each row array, Mix Columns method randomizing data in columns, and AddRoundKey XOR process between states that occur with its round key.
c. Final Round is the final round process using the SubBytes, ShiftRows, AddRoundKey methods.

2.5. Combination of Blockchain and Advanced Encryption Standard (AES) Cryptography

The modification in this study utilizes the Blockchain chain combined with the AES Cryptography method, shown in Figure 6.

p-ISSN: XXXX-YYYY
e-ISSN: XXXX-YYYY

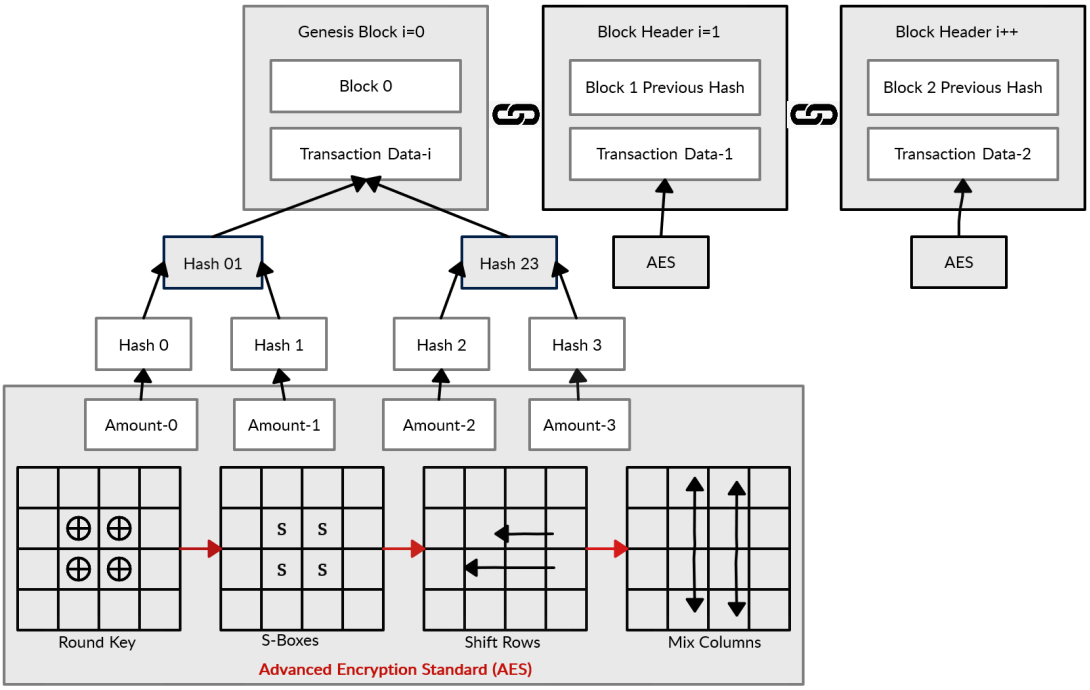


Figure 6. AES Blockchain Modification

Explanation in Figure 6. The blockchain in each block contains information from each student who makes top-up transactions and other transactions. Of course, the transaction is changed in the form of a hash, but in this study using the parameter amount (top-up value in rupiah) to perform the cryptographic process with AES. Applies to each chain in the transaction, because the amount is prone to attacks to avoid a difference in the value of both the initial transaction and the total.

2.6. Testing

a. Cross-Site Scripting (XSS)

Cross-Site Scripting is also known as an injection attack from Cross Scripting, where the attack inserts the attack command code script on a website [26]. The attacker will change the data by hijacking the session, attacking cookies to cause data consistency [27]. So that this research will utilize the XSS scenario in attacking transactions, then perform a validation test on the blockchain.

b. Chain Validation

This test validates the chain on each blockchain, to detect changes in each block by verifying the hash associated with the previous and next block [28][29]. Valid chains will produce true output that is true without any changes and invalid chains will give false output indicating an attack from unauthorized parties. In checking the validation, the researcher utilizes a script from Proof of Work, which is a computational method commonly used for Blockchain technology [30].

3. Result and Discussion

3.1. School Transaction with Top Up

a. Use Case Diagram

p-ISSN: XXXX-YYYY
e-ISSN: XXXX-YYYY

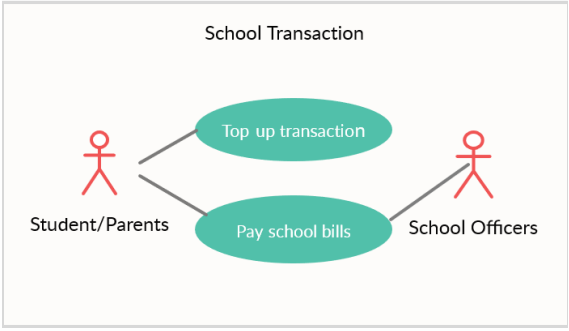


Figure 7. Use Case School Transaction Diagram

Use Case diagram illustrates the relationship between the parties of students both parents or guardians and the school and the school transaction system according to Figure 7. The interaction made by the students is a digital pocket money top-up transaction that can be used to pay school bills. Then the payment will be followed up by the school. This transaction requires protection.

b. Database Design

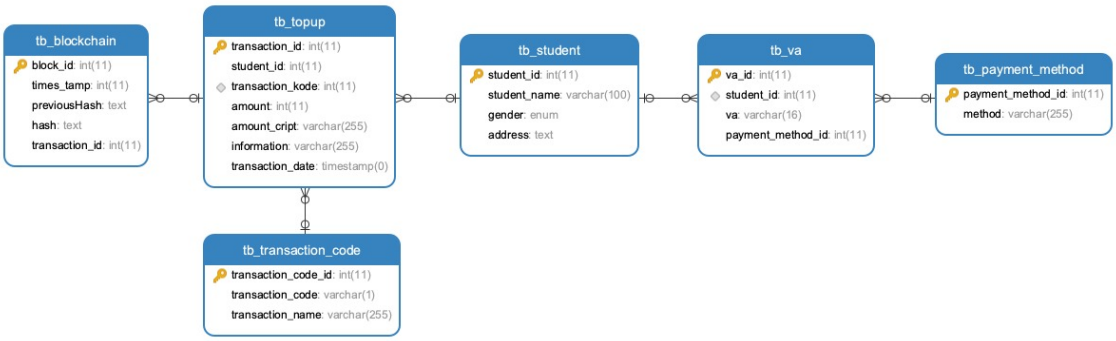


Figure 8. Database Design Top Up with Blockchain-AES

In the blockchain table is a combination Blockchain approach process with AES that is related to the top-up table, where one top-up transaction made by the student is related to each block so that the process that occurs when witness transactions are always recorded and processed by Blockchain-AES. The students can conduct transactions top up many times. Payment methods can only be done with a Virtual Account (VA) because it is easier, faster, and more practical. VA is given to students in a unique form and nominal according to the desired top-up. Each top-up transaction has a record indicating the addition and reduction of the balance in the allowance where the information will be monitored and followed up by the school.

c. User Interface Design

Figure 9. Payment Simulator Top-Up Transaction

p-ISSN: XXXX-YYYY
e-ISSN: XXXX-YYYY

Each student has a unique code in the form of VA which is used in transactions according to Figure 9. If you are going to make a transaction, it will appear in Figure 10.

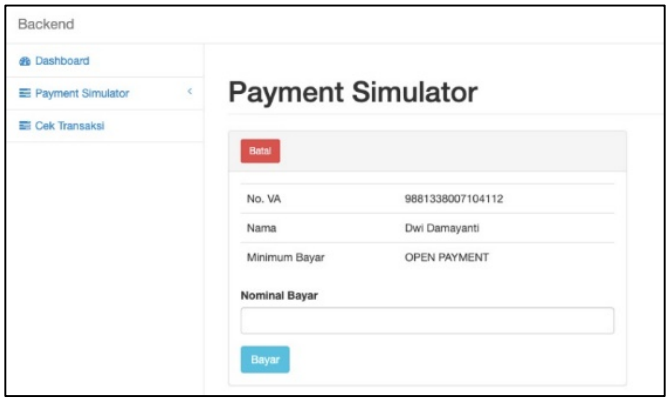


Figure 10. Interface Simulator Top Up by Students

The display on the student side is like Figure 10, the student who will do the top-up is provided with an open payment field and adjusts the nominal top-up that will be done.

3.2. Transaction Top-Up System Design

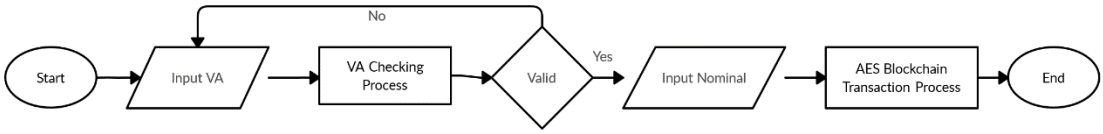


Figure 11. Alur Kerja Transaksi Top

It is shown in Figure 11. In the design of the procedure for a top-up of pocket money transactions, the students do top up with the VA listed then the system checks if the VA is valid then it will continue to be able to enter the top-up nominal. In the transaction process that occurs, the Blockchain-AES approach process is carried out.

3.3. Implementation of Modified Blockchain Technology with Cryptography Advanced Encryption Standard (AES)


```
{
    "status": "00",
    "message": "success",
    "name": "Dwi Damayanti",
    "amount_total": "Rp. 650,000",
    "result": {
        "chain": [
            {
                "nonce": 0,
                "index": 0,
                "timestamp": 1587747600,
                "data": "Genesis Block",
                "previousHash": null,
                "hash":
"558fdb114cbcef913ed07f45c2f644ea5cabc953eef5884a910195b30742c300"
            },
            {
                "nonce": 29,
                "index": 1,
                "timestamp": "1602598649",
                "data": "SeiiBlLqNXokldSU7mMGVw==",
```

p-ISSN: XXXX-YYYY
e-ISSN: XXXX-YYYY


```
                "previousHash":
"558fdb114cbcef913ed07f45c2f644ea5cabc953eef5884a910195b30742c300",
                "hash":
"0c612d1f67db6234bb26c6cf1c418e17658b027c4cd994dd914f5f4b542c27eb"
            },
            . . .
        ],
        "difficulty": 1
    }

}
```


Figure 12. API Response Top Up

Figure 12. is the result of response API when successful conduct transactions top up money pocket. Status 00 in the source code in Fig. 8 indicates the success of the transaction, on behalf of “Dwi Damayanti” top up with a total transaction balance of 650,000 IDR. In the first chain, it is initiated with the Genesis Block, then the value in the "data" chain represents the amount or value of the top-up transaction that has undergone the AES cryptography process then continues to the next chain which is connected to the previous hash before which is chained with the next hash. The implementation of this proposed method uses the PHP programming language CodeIgniter which generates an API response.

3.4. Testing Scenario

a. Cross-Site Scripting (XSS) Attack

Scenario testing an attack on the system is using XSS is to deliberately insert a script that can change the data of transactions specific to the system when it is executed. The scenario for which the attack is performed on the 'amount' data. In this scenario, the attacker has succeeded in changing the security of his transaction data, without knowing the actual amount because it is encrypted.

Table 2. Transaction Data Conducted by Students (Top-up)

Transac-tion ID	ID Stu-dents	Name	Transac-tion	Amount	Info	Transaction Date
1.	4112	Dwi Damayanti	Income	Rp. 50.000	Top Up	2020-10-13 21:17:29
2.	4112	Dwi Damayanti	Income	Rp. 50.000	Top Up	2020-10-13 21:22:19
3.	4112	Dwi Damayanti	Income	Rp. 250.000	Top Up	2020-10-13 21:32:35
4.	4112	Dwi Damayanti	Income	Rp. 150.000	Top Up	2020-10-13 21:49:43
5.	4112	Dwi Damayanti	Income	Rp. 50.000	Top Up	2020-10-13 21:54:26
6.	4112	Dwi Damayanti	Income	Rp. 100.000	Top Up	2020-10-13 22:05:26

Shown in Table 2. is the transaction data conducted by students on behalf of Dwi Damayanti, where the top-up of the transaction has been recorded in the database server according to the transaction date and according to the top-up value. The scenario (see table 3) was performed by the attacker and the data was changed in the third transaction.

Table 3. Modified Attacker Data Scenarios

Test Parameters							
Transac-tion ID	Amount	Status	Message	ID Students	Name	Transac tion	Amount Total
3	300.000	00	Success	4112	Dwi Damayanti	Income	700.000
4	5.000.000	00	Success	4112	Dwi Damayanti	Income	5.550.000
5	300.000	00	Success	4112	Dwi Damayanti	Income	5.800.000
6	100.000	00	Success	4112	Dwi Damayanti	Income	5.800.000

Table 3. is the attack scenario on transaction id 3, where the attacker changes the transaction to 300,000 IDR. The total amount was obtained to be 700,000 IDR because previously in the user database under the name “Dwi Damayanti” 650,000 IDR were stored according to the actual data. The calculation is that on transaction ID 3 the actual data value (according to table 2) is 250,000 IDR then the attacker (see table 3) fills in the amount of 300,000 IDR, then the difference is 50,000 IDR. The difference is added to the total amount of the actual data, then

p-ISSN: XXXX-YYYY
e-ISSN: XXXX-YYYY

the attacker data will add the total amount to 700,000 IDR. So that the amount of data affects the next chain.

b. Chain Validation

This test needs to be done to determine the successful performance of Blockchain technology modification with cryptography. Scenario testing on the system is using a chain validation that will correct the blocks one by one to match the previous hash of the block before. Chain valid will produce output true and chain is not valid will provide output false.

Table 4. Chain Validation Test Results

Index	Timestamp	Data			Amount	Previous Hash	Hash	Valid
		Transaction ID	Transaction Code	Information				
0	1587747600	Null	Null	Null	Genesis Block	Null	558fdb1144...	true
1	1602598649	1	1	Top Up	SeiiBll...	558fdb1144...	Oc612d1f6...	true
2	1602598939	2	1	Top Up	SeiiBll...	Oc612d1f6...	007ce0918...	true
3	1602599555	3	1	Top Up	aX/+0kf...	007ce0918...	0355789ac...	false
4	1602600583	4	1	Top Up	6/9CLU...	0355789ac...	0b59b0b2d...	false
5	1602601462	5	1	Top Up	aX/+0kf...	0b59b0b2d...	030d2e016...	false
6	1602601526	6	1	Top Up	hTx63b...	030d2e016...	0047e66bd...	false

The results of the p chain validation test are in Table 4. shows that the performance of this cryptographic modification of Blockchain technology is working properly on this system. This is evidenced in the success of the chain validation to detect whether there is the immutability of data or not shown on the valid column valuable true or false.

4. Conclusion

The performance of blockchain technology with a combination of AES cryptography can be applied to online transactions to top up pocket money in schools. The use of a centralized blockchain can save costs in using servers, but double security can be provided, namely by involving AES cryptography. The test scenario involves the insertion of the script with Cross-Site Scripting (XSS) attacks, an attacker must first perform a cryptographic process to find out the actual top-up value of the transaction. In chain validation testing, it can be seen that what chain has been attacked, so that changes can be identified.

References

[1] J. Dilley, A. Poelstra, J. Wilkins, M. Piekarska, B. Gorlick, and M. Friedenbach, “Strong Federations: An Interoperable Blockchain Solution to Centralized Third Party Risks,” *CoRR*, vol. abs/1612.0, pp. 1–14, 2016, [Online]. Available: http://arxiv.org/abs/1612.05491.

[2] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview,” *CoRR*, vol. abs/1906.1, pp. 1–57, 2019, [Online]. Available: http://arxiv.org/abs/1906.11078.

[3] R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and A. Singh, “Empirical Vulnerability Analysis of Automated Smart Contracts Security Testing on Blockchains,” *CoRR*, vol. abs/1809.0, pp. 103–113, 2018, [Online]. Available: http://arxiv.org/abs/1809.02702.

[4] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in internet of things: Challenges and Solutions,” *CoRR*, vol. abs/1608.0, pp. 1–13, 2016, [Online]. Available: http://arxiv.org/abs/1608.05187.

[5] N. M. Kumar and P. K. Mallick, “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.

[6] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, “How digital identity on blockchain can contribute in a smart city environment,” *2017 Int. Smart Cities Conf. ISC2 2017*, vol. 00, no. c, pp. 1–4, 2017, doi: 10.1109/ISC2.2017.8090839.

[7] T. G. N. R. Alamelu and R. Soundararajan, “Cryptography Using Neural Network,” *Proc. INDICON 2005 An Int. Conf. IEEE India Counc.*, vol. 2005, no. I, pp. 258–261, 2005, doi: 10.1109/INDCON.2005.1590168.

[8] S. D. Putra, M. Yudhiprawira, S. Sutikno, Y. Kurniawan, and A. S. Ahmad, “Power analysis attack against encryption devices: a comprehensive analysis of AES, DES, and BC3,” *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 17, no. 3, p. 1282, 2019, doi: 10.12928/telkomnika.v17i3.9384.

[9] S. Man and S. Shrestha, “C ++ Implementation of Neural Cryptography for Public Key Exchange and Secure Message Encryption with Rijndael Cipher,” *Academia.Edu*, pp. 1–8, 2013, [Online]. Available: http://www.academia.edu/4055547/NeuroCrypto_C_Implementation_of_Neural_Cryptography_for_Public_Key_Exchange_and_Secure_Message_Encryption_with_Rijndael_Cipher.

[10] R. M. Awangga, “Peuyeum: A Geospatial {URL} Encrypted Web Framework Using Advance Encryption Standard-Cipher Block Chaining Mode,” *{IOP} Conf. Ser. Earth Environ. Sci.*, vol. 145, p. 12055, Apr. 2018, doi: 10.1088/1755-1315/145/1/012055.

[11] A. C. Nugraha, “Penerapan Teknologi Blockchain dalam Lingkungan Pendidikan,” *J. PRODUKTIF*, vol. 4, no. 1, pp. 15–20, 2020.

[12] H. F. Putra and O. Penangsang, “Penerapan Blockchain dan Kriptografi untuk Keamanan Data pada Jaringan Smart Grid,” *J. Tek. ITS*, vol. 8, no. 1, pp. 11–16, 2019.

[13] A. Winarno, “Desain e-Transkip dengan Teknologi Blockchain,” *Semin. Nas. Paker ke 2*, pp. 1–6, 2019.

[14] M. D. K. Perdani, Widyawan, and P. I. Santosa, “Blockchain Untuk Keamanan Transaksi Elektronik Perusahaan Financial Technology (Studi Kasus Pada PT XYZ),” *Semin. Nas. Teknol. Inf. dan Multimed.*, pp. 7–12, 2018.

[15] M. Benchoufi and P. Ravaud, “Blockchain technology for improving clinical research quality,” *Trials*, vol. 18, no. 1, pp. 1–5, 2017, doi: 10.1186/s13063-017-2035-z.

[16] D. Efanov and P. Roschin, “The all-pervasiveness of the blockchain technology,” *Procedia Comput. Sci.*, vol. 123, pp. 116–121, 2018, doi: 10.1016/j.procs.2018.01.019.

[17] A. Wright and P. De Filippi, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia,” *Br. Poult. Sci.*, vol. 14, no. 2, pp. 149–152, 2015, doi: 10.1080/00071667308416007.

[18] M. Shabani, “Blockchain-based platforms for genomic data sharing: a de-centralized approach in response to the governance problems?,” *J. Am. Med. Informatics Assoc.*, vol. 26, no. 1, pp. 76–80, 2019, doi: 10.1093/jamia/ocy149.

[19] D. L. K. Chuen, *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. Academic Press, 2015.

[20] R. Henry, A. Herzberg, and A. Kate, “Blockchain access privacy: Challenges and directions,” *IEEE Secur. Priv.*, vol. 16, no. 4, pp. 38–45, 2018, doi: 10.1109/MSP.2018.3111245.

[21] P. Mahajan and A. Sachdeva, “A Study of Encrytion Algorithms AES, DES and RSA for Security,” *Exp. Mech.*, vol. 13, no. 15, p. 9, 2013, doi: 10.1007/BF02322384.

[22] D. A. Meko, “Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu,” *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 8–15, 2018.

[23] G. W. Bhaudhayana and I. M. Widiartha, “Implementasi algoritma kriptografi aes 256 dan metode steganografi lsb pada gambar bitmap,” *J. ilmu Komput. Univ. Udayana*, vol. 8, no. 2, pp. 15–25, 2015.

[24] R. K. Meenakshi and A. Arivazhagan, “RTL Modelling for the Cipher Block Chaining Mode (CBC) for Data Security,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 8, no. 3, pp. 709–711, 2017, doi: 10.11591/ijeecs.v8.i3.pp709-711.

[25] A. Nugrahantoro *et al.*, “Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC),” vol. XII, no. 1, pp. 12–21, 2020.

p-ISSN: XXXX-YYYY
e-ISSN: XXXX-YYYY

[26] R. Firmansyah and W. S. Prasetya, “Pencegahan Serangan Cross Site Scripting dengan Teknik Metacharacter pada Sistem e-Grocery,” *J. ENTER*, vol. 1, no. Agustus, pp. 294–306, 2018.

[27] G. E. Rodríguez, J. G. Torres, P. Flores, and D. E. Benavides, “Cross-site scripting (XSS) attacks and mitigation: A survey,” *Comput. Networks*, vol. 166, p. 106960, 2020, doi: https://doi.org/10.1016/j.comnet.2019.106960.

[28] D. Deuber, B. Magri, and S. A. K. Thyagarajan, “Redactable blockchain in the permissionless setting,” *Proc. - IEEE Symp. Secur. Priv.*, vol. 2019-May, pp. 124–138, 2019, doi: 10.1109/SP.2019.00039.

[29] N. Alzahrani and N. Bulusu, “Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain,” in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 2018, pp. 30–35, doi: 10.1145/3211933.3211939.

[30] G. Kumar, R. Saha, M. K. Rai, R. Thomas, and T. H. Kim, “Proof-of-Work Consensus Approach in Blockchain Technology for Cloud and Fog Computing Using Maximization-Factorization Statistics,” *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6835–6842, 2019, doi: 10.1109/JIOT.2019.2911969.

Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 4, No. 3, August 2019, Pp. 197-206

Internet of thing (IoT) security optimization against cross-site scripting (XSS) attacks based on blockchain technology

Imam Riadi*[1], Rusydi Umar[2], Tri Lestari[3]
Department of Information System Universitas Ahmad Dahlan Yogyakarta, Indonesia[1]
Departmen of Informatics Universitas Ahmad Dahlan Yogyakarta, Indonesia[2,3]

Article Info
Keywords:
IoT, XSS, Security, Blockchain

Article history:

Cite:

*Corresponding author.
Imam Riadi
E-mail address:
imam.riadi@is.uad.ac.id

Abstract
One of the technologies that emerged in the era of the 4.0 industrial revolution is the internet of things (IoT). IoT in this study is used as a medium for sending payment transaction data so that it can be stored on the REST API server. Transaction data sent using IoT is very vulnerable to various types of attacks if it is not secured, one of which is vulnerable to cross-site scripting (XSS) attacks. Hackers can steal, change, and even delete payment transaction data that IoT has sent in the REST API so that security needs to be improved. Security optimization in this study was carried out by implementing blockchain. Blockchain, which has the advantage the security, is expected to be able to secure payment transaction data stored in the REST API. This research was carried out in several stages, first the collection of research tools, second IoT planning, third vulnerability testing, fourth blockchain implementation and, finally vulnerability testing after blockchain implementation. The results obtained from this study are the implementation of blockchain to increase security on IoT payment transactions to avoid successful XSS attacks. Evidenced by the results of payment transaction IoT vulnerability testing before and after blockchain implementation, prior to blockchain implementation, the payment transaction IoT vulnerability testing results stated that 1 XSS vulnerability was found which had a high level of overall risk, while the results of vulnerability testing after blockchain implementation were not found a vulnerability from an XSS attack (its XSS vulnerability gap was 0 or not found).

1. Introduction

The digital era is an age where everyone has used technology and they are connected easily. The digital era appears due to technology that is developing so rapidly [1]. One of the emerging technologies and its development that has recently become a hot topic in the era of the 4.0 industrial revolution is the internet of things (IoT) [2]. IoT is a computing concept about objects in daily life that are connected to the internet and able to identify themselves to other devices. IoT does not only have the potential to influence lifestyle but also how it works [3]. The concept of IoT includes 3 main elements, namely: physical or real objects that have been integrated on the sensor module, internet connection, and data centers on servers to store data or information from applications [4]. The use of objects that are connected to the internet will collect data which is then collected into big data to be processed and analyzed by government agencies, related companies, and other agencies and then used for their respective interests [5]. IoT has several advantages including, IoT can improve user experience, increase device usage and help improve technology to make it more effective in its use [6]. One example of IoT which is also used as the object of this research is the payment transaction IoT, where this IoT is used to send transaction data entered from the system to the API rest server [7]. IoT is made to facilitate application developers in the process of storing data input from the system and stored on the server, with the IoT data storage to the server becomes more effective [8].

IoT does provide many benefits if implemented, but IoT is also not spared from various shortcomings, one of the disadvantages of IoT is on the security side [9]. The ecosystem of devices created by IoT is constantly connected and communicates with each other via a network, which is why users are exposed to various types of attacks [10]. Therefore, every IoT that is designed must be equipped with security to avoid various types of attacks such as cross-site scripting (XSS), SQL injection, and other malicious attacks [11] [12]. The IoT payment transactions that are used as objects in this research are not equipped with system security, so in this study, an optimization of the IoT payment transaction security is carried out to avoid attacks, especially cross site scripting (XSS) [13] [14]. XSS is a type of code injection attack carried out by an attacker by entering HTML code. XSS attacks can result in security on the client-side

being bypassed so that attackers can steal, modify and even delete payment transaction data that IoT sends to the REST API [15].

Optimization of IoT payment transaction security in this study will be carried out using blockchain technology. Technology that has the advantage of security is currently being discussed, blockchain is a distributed database that is used to maintain a growing list of records, also known as blocks, in this research blockchain plays a role in securing payment transaction data stored in the REST API so that transaction data which is stored safely and can avoid XSS attacks [16]. Figure 1 is an example of how blockchain works.

.

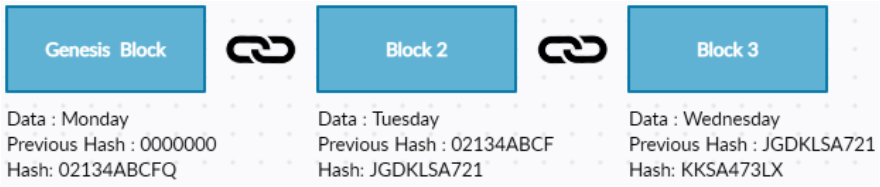


Figure 1. How Blockchain works

Figure 1 shows each block on the blockchain network containing the link and timestamp of the previous block [17]. Blockchain is managed by a peer to peer network that collectively adheres to protocols to validate new blocks [18]. Blockchain is very suitable for securing IoT payment transactions because blockchain technology is safe, transparent and, immutable [19]. Blockchain also uses consensus algorithms which are useful for reaching an agreement on a single data value [20]. The consensus algorithm is mechanistic and automatically synchronizes all transaction data in the blockchain [21]. Three popular consensus algorithms include proof of work (PoW), Proof of Stake (PoS), and Delegate Proof of Stake (DPoS) [22]. This study uses a consensus Proof of Work (PoW) algorithm which requires solving complex math in cryptography through a node on the network so that it runs long and random process of presenting answers to basic experiments and errors [23].

2. Research Method

This research will be conducted in several stages, the first stage is the collection of research equipment. The tools needed in the first study were used for IoT design including NodeMCU, RS232, USB cable, and laptop. Second, the tool used for vulnerability testing is the XSS Vulnerability Scanner software. The three tools used for blockchain planning and implementation are VisualStudio software. The following is a brief explanation regarding the tools used in the study.

1. NodeMCU can be analogous to the Arduino board of the ESP826 and has also packaged the ESP8266 into a compact board with various features like a microcontroller plus the ability to access Wifi as well as a USB to serial communication chip, so for programming only a USB data cable extension is required such as used in the data cable and charging cable for Android smartphones [24]. The NodeMCU used in this study can be seen in Figure 2.

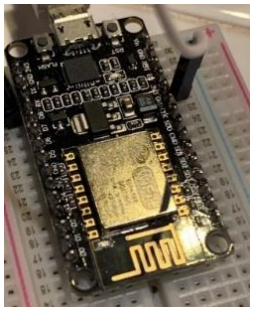


Figure 2. NodeMCU for designing IoT

The advantages of NodeMCU include low cost, integrated support for WiFi networks, a smaller board size, and lower energy consumption. Following are the basic specifications of NodeMCU; Tensilica 32bit Microcontroller, 4KB Flash Memory, 3.3V Operating Voltage, 7-12V Input Voltage, Digital I / O 16, Analog Input 1 (10 Bit), Interface UART 1, Interface SPI 1, Interface I2C 1. How to install NodeMCU programmed, the micro USB cable is connected to the NodeMCU USB port and a laptop USB port connected to the internet so that the download process can be carried out, if it is detected on the computer you will see USB-SERIAL CH340 on the device manager, for the com number it can be different on each computer.

2. RS232 is a data transmission series communication standard between two electronic devices. Serial data communication is done by sending data bit by bit sequentially. RS232 can be seen in Figure 3.

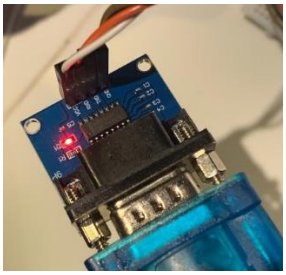


Figure 3. RS232 for designing IoT

Figure 3 is the RS232 used in the study, RS232 has been connected to a laptop using an HDMI to VGA cable and NodeMCU is connected with a cable that has been adjusted.

3. USB and laptop, these two tools are used to assist the IoT design process, as previously explained, RS232 must be connected to the laptop using a USB cable so that the input data can be read and processed by RS232 and NodeMCU.
4. XSS Vulnerability Scanner is a vulnerability testing tool for web applications and network infrastructure that is strong and strongly integrated so that with this tool, vulnerability testing becomes more effective and easy [25] [26].
5. VisualStudio is used to design blockchain using the node.js programming language.

After the research tools are collected, it is continued with IoT design. IoT that is designed and connected to data, is tested for vulnerability using the XSS Vulnerability Scanner to find vulnerabilities, especially from XSS attacks. If a vulnerability is found in the IoT, a blockchain is implemented to increase its security. After the blockchain implementation has been successfully carried out, it is continued with another vulnerability testing to prove whether the blockchain implementation to secure the IoT was successful. The flow carried out in this study can be seen in Figure 4.

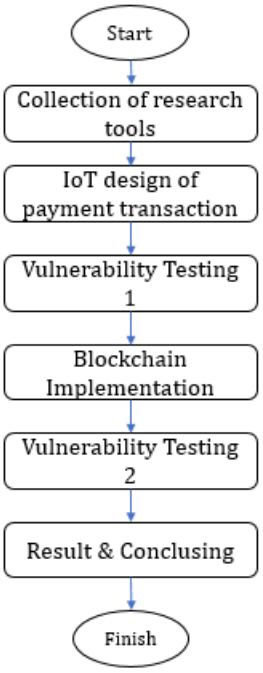


Figure 4. Research Methodology

Figure 4 is the flow or stages of the research carried out. First, research tools are collected, followed by IoT planning, after which vulnerability testing is carried out, followed by blockchain implementation and carried out with vulnerability testing after blockchain implementation, ending with drawing results and conclusions.

3. Results and Discussion

This section shows the Payment Transaction IoT optimization process from an XSS attack. The first stage is the collection of research tools. The second stage of IoT design uses RS232 and NodeMCU. The third stage is vulnerability testing before optimization is carried out. The fourth stage of blockchain implementation. The fifth stage of vulnerability testing after optimization is carried out.

The first is the collection of equipment, the tools needed in this study can be seen in Table 1.

Table 1. Tools

No	Name	Category	Information
1	NodeMCU	Hardware	To design the IoT
2	RS232	Hardware	To design the IoT
3	Cable USB	Hardware	To design the IoT
4	Laptop	Hardware	To design the IoT
5	XSS Vulnerability Scanner	Software	For Pentes
6	VisualStudio	Software	For design Blockchain

Table 1 contains the research tools needed in research. Number 1 is the NodeMCU which is used to design the IoT. Number 2 is RS232 which is used to change the data entered by the user so that it can be read by NodeMCU. Numbers 3 and 4 are USB cables and laptops, both of these tools are used to assist the IoT design process. Number 5 XSS Vulnerability Scanner to test the vulnerability of payment transactions IoT. Number 6 VisualStudio is used to design a blockchain that will be implemented in the payment transaction IoT.

Second, the design of payment transaction IoT which is used as a demonstration of sending cryptocurrency transaction data. The device is set up so that it can send data through sensors, namely data on the sender, receiver and nominal amount sent. IoT is designed using NodeMCU assisted by RS232. The IoT design in this study can be seen in Figure 5.

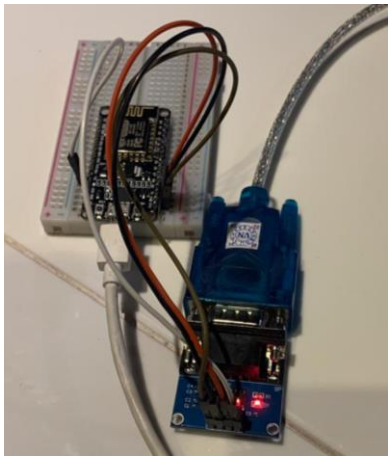


Figure 5. Payment Transaction IoT Design

Figure 5 is an RS232 image that is connected to NodeMCU using a cable with the rules as described in Table 2.

Table 2. RS232 to NodeMCU cable management

RS232	Connected	NodeMCU
GND	------→	GND
VCC	------→	3V3
RXD	------→	RX
TXD	------→	TX

Table 2 describes the cable arrangement for connecting RS232 with NodeMCU, where GND on RS232 is connected to GND on NodeMCU, VCC is connected to 3V3, RDX with RX, and TXD with TX. Data transmission from RS232 can be done in one or two directions, the data transfer rate is quite low, the maximum is only 19200 bits per second. Then for the complete IoT design, it can be seen as in Figure 6.

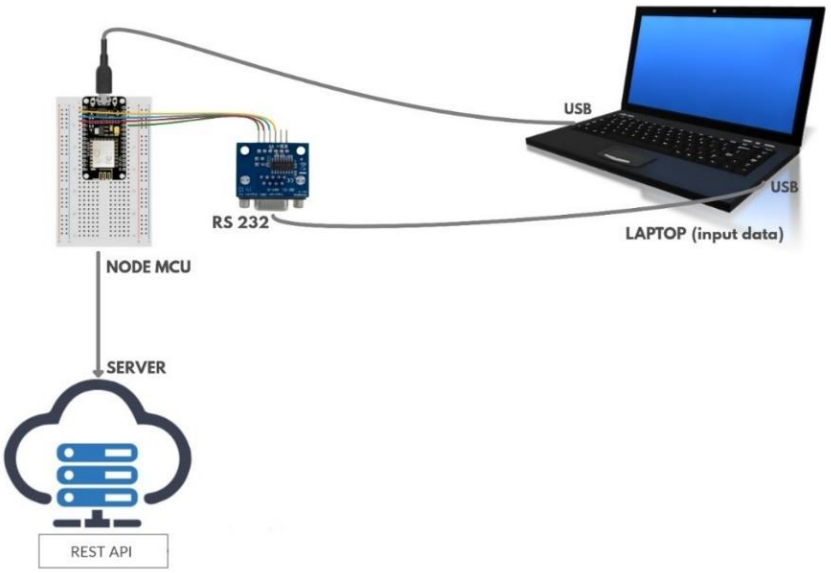


Figure 6. Payment Transaction IoT Design

Figure 6 shows a laptop connected to RS232 and NodeMCU. Laptops are used to send virtual account data and amounts. The data is received by RS232 to be converted first, then the results are then sent to NodeMCU for embedded c ++ code in which there are transaction data settings, URL end front Rest API, and API configuration. Data that has been installed in NodeMCU can be sent directly to the server.

Third, the vulnerability testing in the study was carried out twice, the first test was before the blockchain implementation and the second test was carried out after the blockchain implementation. This vulnerability testing is carried out using XSS Vulnerability Scanning, and the results of the first vulnerability testing can be seen in Figure 7.

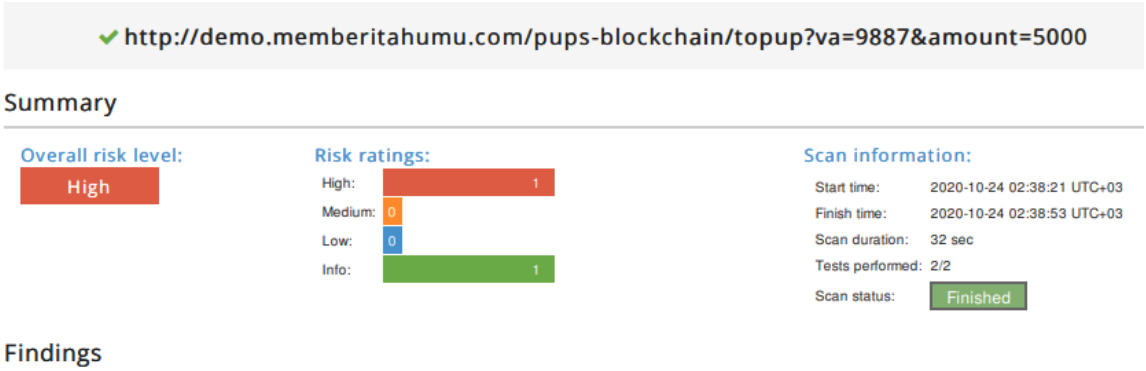


Figure 7. Vulnerability Testing Results

Figure 7 shows a summary of vulnerability testing on the webserver demo.memberumu.com/pups-blockchain. The report from the results of the vulnerability testing shows that the webserver has 1 vulnerability in XSS which has a high level of overall risk. This shows that the security of IoT payment transactions must be increased so that it can avoid XSS attacks.

Fourth, blockchain implementation is carried out to increase security on payment IoT, namely API data stored in the demo.memberitahumu.com/pups-blockchain webserver. The blockchain implementation process can be seen in Figure 8.

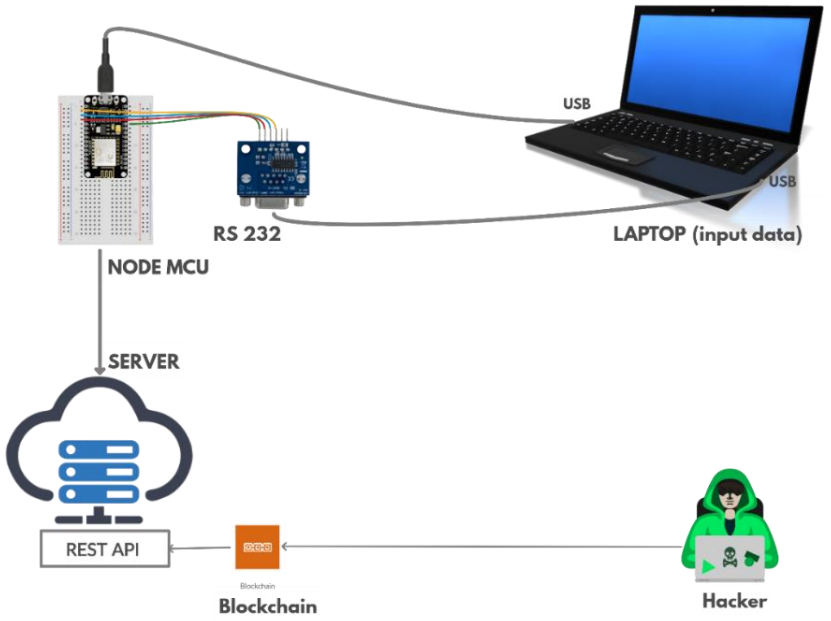


Figure 8. *Blockchain Implementation*

Figure 8 explains that blockchain is applied to the web server REST API, this is so that the blockchain can prevent various XSS attacks that are sent. The following is a program listing on the REST API payload after the blockchain is implemented.


```
"status": "00",
    "message": "success",
    "name": "Dani Saputra",
    "amount_total": "Rp. 225,000",
    "result": {
        "chain": [

{
  "nonce": 0,
  "index": 0,
  "timestamp": 1587747600,
  "data": "Genesis Block",
  "previousHash": null,
  "hash":"558fdb114cbcef913ed07f45c2f644ea5cabc953eef5884a910195b30742c300"
  },

{
  "nonce": 13,
  "index": 1,
  "timestamp": "1603195046",
  "data": "50000",
  "previousHash":"558fdb114cbcef913ed07f45c2f644ea5cabc953eef5884a910195b30742c300",
  "hash":"07736a69c442aaf9f78fcf9288c6e94587647c399e643565d6fef4342e71021f"
  },

{
  "nonce": 9,
  "index": 2,
   "timestamp": "1603197946",
   "data": "75000",
  "previousHash":"07736a69c442aaf9f78fcf9288c6e94587647c399e643565d6fef4342e71021f",
  "hash":"0ba9e86bf8644825085d391284baf24c0188da1d9d4203d553bc0b6281ded6a8"
  },

{
  "nonce": 15,
  "index": 3,
   "timestamp": 1603199769,
  "data": "100000",
  "previousHash":"0ba9e86bf8644825085d391284baf24c0188da1d9d4203d553bc0b6281ded6a8",
  hash":"04f75880b30ed3f9278a83e8648ba1a8b78c567f0e3906b5946a35413a44c03f"
  }

],
```

```
   "difficulty":
   "status": "00",
   "message": "success",
   "name": "Dani Saputra",
   "amount_total": "Rp. 225,000",
   "result": [

{
   "amount": "50000"
   },
{
   "amount": "75000"
   },
{
   "amount": "100000"
}
]
}
```


The data sent in the form of name and amount of money are then made into a block. Each block on the blockchain contains the timestamp, data, previous hash, and hash itself. The first block is called the genesis block, contains transaction data with a previous hash that is still null and generates a hash for the block itself, as well as the next block, it's just that the difference is that the contents of the previous hash are no longer null and the respective hash values. block. Payment transaction data entered by users can be seen and read by all connected members in the blockchain network. The blockchain implementation will synchronize all payment transaction data made by IoT devices. Each member on the blockchain network has a key pair to make transactions. Every data input becomes a block that is connected to become a chain therefore every member is not allowed to change or delete every block of data. The chain containing interconnected block blocks will be carried out consensus so that blocks containing invalid data can be ignored by other members and even deleted from the blockchain network automatically. Each block with a transaction value that is different from the majority value in a blockchain network will be eliminated and the value stored in each blockchain member data is repaired, therefore if an attacker tries to change the transaction data on the blockchain network it will be eliminated and the data collected changed will be repaired automatically.

Fifth, vulnerability testing is carried out again after the blockchain implementation is carried out, this aims to prove whether the blockchain implementation to increase IoT payment transactions has been successfully carried out. The results of this vulnerability testing can be seen in Figure 9.

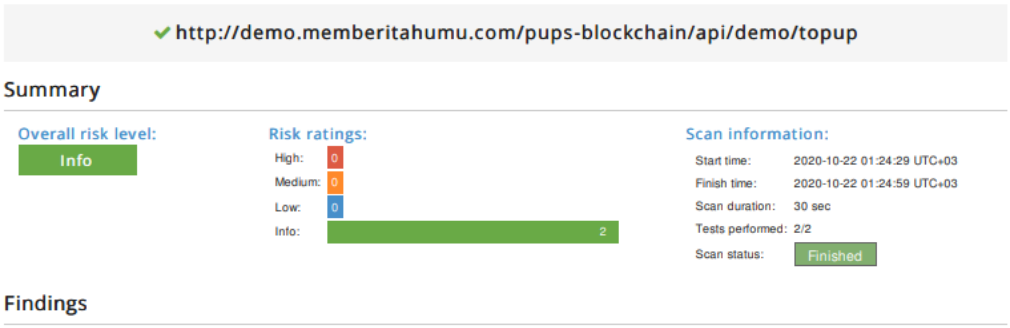


Figure 9. Vulnerability Testing Results after Blockchain Implementation

Figure 9 shows the results of vulnerability testing after blockchain implementation is carried out, the results of the vulnerability testing show the overall level of risk is the absence of vulnerabilities from XSS attacks, this shows that the optimization of IoT security for payment transactions using blockchain is 100% successful.

4. Conclusion

Security on IoT payment transactions needs to be considered in the digital era like today, increasingly fast technology can increase digital crime which is getting faster too. One of the ways to improve IoT is by implementing blockchain as was done in this research. Blockchain implementation to secure IoT payment transactions in this study was successfully carried out, as evidenced by the results of vulnerability testing using the XSS Vulnerability Scanner which was carried out before and after blockchain implementation was carried out. Before blockchain implementation was carried out, the overall risk level was found 1 XSS vulnerability gap which had a high level of overall risk, then the result of vulnerability testing after blockchain implementation was not found vulnerabilities from XSS attacks.

References

[1] I. Riadi *et al.*, "Cross Site Scripting (XSS) Attack Vulnerability Analysis on Smart Payment Applications Using the OWASP Framework," vol. 5, no. 3, pp. 146–152, 2020. http://ejournal.uin-suka.ac.id/saintek/JISKA/article/view/1851/1783

[2] J. Fat, H. Candra, and W. Wiliam, "Sensor Data Securitization in Internet of Things (IoT) Applications Using the Ethereum Blockchain on the Testnet Network," *TESLA J. Tek. Elektro*, vol. 21, no. 1, p. 79, 2019, doi: 10.24912/tesla.v21i1.5886. https://www.researchgate.net/publication/337164682_Sekuritisasi_Data_Sensor_Pada_Aplikasi_Internet_of_Things_IoT_Dengan_Menggunakan_Blockchain_Ethereum_Di_Jaringan_Testnet

[3] L. Arief and T. A. Sundara, "Studies on the Use of Blockchain for the Internet of Things (IoT)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 1, no. 1, p. 70, 2017, doi: 10.29207/resti.v1i1.26. https://www.researchgate.net/publication/321798741_Studi_atas_Pemanfaatan_Blockchain_bagi_Internet_of_Things_IoT

[4] D. Sasmoko and Y. A. Wicaksono, "IImplementing the Application of the Internet of Things (IoT) in Infusion Monitoring Using ESP 8266 and WEB to Share Data," *J. Ilm. Inform.*, vol. 2, no. 1, pp. 90–98, 2017, doi: 10.35316/jimi.v2i1.458. https://ejournal.amiki.ac.id/index.php/JIMI/article/view/36/21

[5] Y. Efendi, "Internet Of Things (IoT) Light Control System Using a Mobile-Based Raspberry Pi," *J. Ilm. Ilmu Komput.*, vol. 4, no. 1, pp. 19–26, 2018, doi: 10.35329/jiik.v4i1.48. https://media.neliti.com/media/publications/283803-internet-of-things-iot-sistem-pengendali-c98bdddd.pdf

[6] F. Rozi, H. Amnur, F. Fitriani, and P. Primawati, "Home Security Using Arduino Based on Internet Of Things," *INVOTEK J. Inov. Vokasional dan Teknol.*, vol. 18, no. 2, pp. 17–24, 2018, doi: 10.24036/invotek.v18i2.287. http://invotek.ppj.unp.ac.id/index.php/invotek/article/view/287/72

[7] O. K. Sulaiman and A. Widarma, "Cloud Computing Based Internet of Things (IoT) System in Campus Area Network," 2017, doi: 10.31227/osf.io/b6m79.https://www.researchgate.net/publication/316506717_Sistem_Internet_Of_Things_IoT_Berbasis_Cloud_Computing_dalam_Campus_Area_Network

[8] A. A. Wardana, A. Rakhmatsyah, A. E. Minarno, and D. R. Anbiya, "Internet of Things Platform for Manage Multiple Message Queuing Telemetry Transport Broker Server," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, no. 3, pp. 197–206, 2019, doi: 10.22219/kinetik.v4i3.841. https://kinetik.umm.ac.id/index.php/kinetik/article/view/841/pdf

[9] A. A. Kristanto, Y. Harjoseputro, and J. E. Samodra, "Golang and New Simple Queue Implementation on Third Party Sandbox System Based on REST API," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 745–750, 2020. https://jurnal.iaii.or.id/index.php/RESTI/article/view/2218/287

[10] T. R. Firdaus and J. T. Informatika, "Web Application Security Through Cross Site Request Forgery (CSRF) Implementation," 2016. https://docplayer.info/194333905-Keamanan-aplikasi-web-melalui-penerapan-cross-site-request-forgery-csrf.html

[11] S. S. H. Putra, "Countermeasures for XSS Attacks, CSRF, SQL Injection Using Blackbox Methods on the IVENMU Marketplace," *J. Pendidik. dan Teknol. Inf.*, vol. 4, no. 2, pp. 289–300, 2017. http://lppm.upiyptk.ac.id/PTI/index.php/pti/article/view/75

[12] A. D. Djayali, "Analysis of SQL Injection Attacks on Online Study Plan Card filling Server (KRS)," vol. 1, no. 1, pp. 1–9, 2020. https://jurnal.aikomternate.ac.id/index.php/jaminfokom/article/view/4/4

[13] Y. Yulianingsih, "Protecting Applications from Cross Site Scripting Attacks with the Metacharacter Method," *J. Nas. Teknol. dan Sist. Inf.*, vol. 3, no. 1, pp. 83–88, 2017, doi: 10.25077/teknosi.v3i1.2017.83-88. https://teknosi.fti.unand.ac.id/index.php/teknosi/article/view/170/85

[14] Rusdiana, C. Banta, and Sanusi, "Website Security Analysis Against Cross-Site Request Forgery (CSRF) Attacks," *KANDIDATJurnal Ris. dan Inov. Pendidik.*, vol. 1, no. 1, pp. 21–29, 2019. https://syekhnurjati.ac.id/journal/index.php/itej/article/download/10/10

[15] A. Y. W, Yunanri, Imama Riadi, "Analysis of Vulnerability Detection on the Open Journal System Webserver Using OWASP Scanner," *Jurnal Rekayasa Teknologi Informasi (JURTI)*, vol. 2, no. 1. pp. 1–8, 2018. http://e-journals.unmul.ac.id/index.php/INF/article/view/1319/pdf

[16] A. C. Nugraha, "Application of Blockchain Technology in the Educational Environment," *J. PRODUKTIF*, vol. 4, no. 1, pp. 15–20, 2020. https://journal.umtas.ac.id/index.php/produktif/article/view/386/336

[17] U. Rahardja, Q. Aini, M. Yusup, and A. Edliyanti, "Application of Blockchain Technology as a Media for Securing E-Commerce Transaction Processes," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 5, no. 1, p. 28, 2020, doi: 10.24114/cess.v5i1.14893. https://www.researchgate.net/publication/342955653_Penerapan_Teknologi_Blockchain_Sebagai_Media_Pengamanan_Proses_Transaksi_E-Commerce

[18] S. D. K. Hu, H. N. Palit, and A. Handojo, "Blockchain Implementation: An e-Voting Case Study," *J. Infra*, vol. 7, no. 1, pp. 183–189, 2019. http://publication.petra.ac.id/index.php/teknik-informatika/article/view/8069/7279

[19] S. Rahmadika, D. R. Ramdania, and M. Harika, "Security Analysis on the Decentralized Energy Trading System Using Blockchain Technology," *J. Online Inform.*, vol. 3, no. 1, p. 44, 2018, doi: 10.15575/join.v3i1.207. https://join.if.uinsgd.ac.id/index.php/join/article/view/v3i17/92

[20] E. P. Harahap, Q. Aini, and R. K. Anam, "Utilization of Blockchain Technology on the Crowdfunding Platform," *Technomedia J.*, vol. 4, no. 2, pp. 199–210, 2019, doi: 10.33050/tmj.v4i2.1108. https://www.researchgate.net/publication/339094728_PEMANFAATAN_TEKNOLOGI_BLOCKCHAIN_PADA_PLATFORM_CROWDFUNDING

[21] H. F. Putra, W. Wirawan, and O. Penangsang, "Application of Blockchain and Cryptography for Data Security on Smart Grid Networks," *J. Tek. ITS*, vol. 8, no. 1, 2019, doi: 10.12962/j23373539.v8i1.38525. http://ejurnal.its.ac.id/index.php/teknik/article/view/38525/5604

[22] A. Argani and W. Taraka, "Utilization of Blockchain Technology to Optimize Certificate Security in Higher Education," *ADI Bisnis Digit. Interdisiplin J.*, vol. 1, no. 1, pp. 10–21, 2020. https://adi-journal.org/index.php/abdi/article/view/121/40

[23] I. Riadi, R. Umar, and I. Busthomi, "Man in the Middle Attack (MiTM) Authentication Security Optimization Using Blockchain Technology," vol. 04, no. June, pp. 15–19, 2020. https://journal.unesa.ac.id/index.php/jieet/article/view/7953/pdf

[24] R. Doni and M. Rahman, "Iot-Based Hydroponic Plant Monitoring System (Internet of Thing) Using Nodemcu ESP8266," vol. 4, no. September, pp. 516–522, 2020. http://ejurnal.tunasbangsa.ac.id/index.php/jsakti/article/view/243/225

[25] L. M. Gultom and M. Harahap, "Analysis of Website Security Gap Analysis of Government Agencies in North Sumatra," *Teknovasi*, vol. 2, no. 2, pp. 1–7, 2015. https://media.neliti.com/media/publications/225752-analisis-celah-keamanan-website-instansi-8f07d7a8.pdf

[26] D. Metasari, F. Irsyadi, and Jatmiko, "Website Security Analysis at the Muhammadiyah University of Surakarta," *Koleks. Karya Ilm. Perpust. Univ. Muhammadiyah Surakarta*, 2014, [Online]. Available: http://eprints.ums.ac.id/28196/21/NASKAH_PUBLIKASI.pdf.

Optimasi Keamanan Autentikasi dari *Man in the Middle Attack* (MiTM) Menggunakan Teknologi Blockchain

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

[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Indonesia
[2,3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan, Indonesia
[1]imam.riadi@is.uad.ac.id
[2]rusydi@mti.uad.ac.id
[3]iqbal1907048011@webmail.uad.ac.id

***Abstrak*— Teknologi informasi memberikan dampak yang besar dalam aspek bisnis. Sistem informasi merupakan salah satu dampak dari kemajuan teknologi yang menjadi salah satu sarana untuk memudahkan pengelolaan informasi dan pelaporan pada sebuah perusahaan. Sistem informasi menggunakan proses autentikasi sebagai gerbang depan untuk melakukan validasi user sebelum mendapatkan layanan. Proses autentikasi memiliki kerentanan dari serangan siber, diantaranya adalah *Man-in-the-middle attack*. *Payload* autentikasi yang dikirim dan diterima pada sebuah sistem informasi perlu diamankan dengan baik. Pengiriman payload autentikasi dalam bentuk *plaintext* rentan akan serangan *Man-in-the-middle*. Teknologi Blockchain memberikan solusi keamanan berupa mekanisme blok hash untuk mengamankan data *payload*. *Payload* autentikasi sebelum dikirmkan diubah menjadi blok hash, sehingga keamanan dan kerahasiaan data payload lebih terjamin.**

***Kata Kunci*— Autentikasi, *Man-in-the-middle attack*, Teknologi Blockchain, Hash, *Payload*.**

I. PENDAHULUAN

Teknologi berkembang dengan sangat pesat, hingga menjadikan teknologi sebagai sarat dalam komunikasi dan berbagi informasi. Kemajuan teknologi memberikan peranan penting dalam memberikan sumber data [1]. Teknologi informasi mengolah data-data yang ada menjadi sebuah informasi.

Teknologi informasi membawa dunia bisnis menjadi lebih ringkas, karena kecanggihan teknologi tak hanya memangkas waktu tetapi juga menjadi perantara komunikasi. Sebagai contoh seperti kantor pos kini tidak lagi relevan karena komunikasi menggunakan jaringan informasi memberikan layanan yang lebih cepat, sehingga kini kantor pos lebih berfungsi sebagai jasa pengantar barang daripada perantara pengiriman surat [2].

Dampak Perkembangan teknologi mengiringi perkembangan perusahaan dan bisnis yang lebih deikenal dengan sebutan *e-commerce*. Kemudahan yang ditimbulkan dari munculnya *e-commerce* mengundang orang-orang yang memiliki jiwa wirausaha kemudian berlomba-lomba mendirikan perusahaan pemula atau biasa di sebut dengan perusahaan *startup*. *Startup* identik dengan pemula bisnis (belum lama beroperasi) dan masih dalam proses pengembangan dalam memilih pasar dari bisnis yang dibangun, tetapi pada kenyataanya *startup* lebih seperti menjadi perusahaan yang bergerak dengan memaksimalkan kinerja teknologi informasi dan internet karena biasanya berfokus pada penggunaan website dan sistem informasi [3].

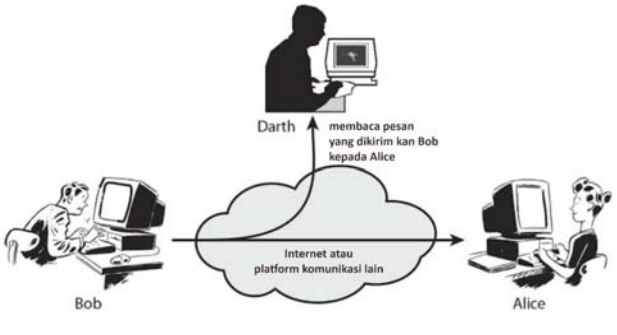
Sistem informasi merupakan sebuah aplikasi yang digunakan dalam sebuah organisasi yang sebagai pendukung pengelolaan transaksi hingga pelaporan [4]. Autentikasi merupakan gerbang utama dalam sebuah sistem informasi, sehingga dapat mendapatkan layanan sesuai dengan hak akses yang diberikan kepada user tersebut [5]. Proses autentikasi merupakan proses validasi user pada saat memasuki sistem dan memungkinkan user untuk mengakses seluruh layanan yang diberikan pleh sistem tanpa perlu memasukkan passwordnya berulang kali [6], [7].

Keamanan informasi merupakan aspek penting yang perlu diperhatikan dalam membangun sistem [6]. Proses autentikasi yang merupakan gerbang depan dalam sebuah sistem informasi memiliki celah dan kerentanan, diantaranya proses pengiriman dan penerimaan *payload* dari server dalam bentuk *plaintext* [7]. Keamanan pada proses autentikasi perlu ditingkatkan guna menanggulagi serangan-serangan siber seperti *Cross Site Scripting* (XSS), *Sniffing*, dan juga serangan *Man-in-the-middle* [8].

Man-in-the-middle attacks adalah salah satu serangan pada jaringan dengan akses terbuka [8]. *Man-in-the-middle attacks* merupakan serangan yang pada dasarnya penyerang memasukkan dirinya di antara dua pihak atau perangkat dalam mode sembunyi-sembunyi sehingga semua paket yang berlintas antara kedua pihak yang sah itu dialihkan melalui penyerang tersebut. Serangan ini cukup berbahaya karena penyerang kemudian dapat mengubah informasi dari paket yang dikirimkan, dan berpotensi mengirim data yang dipalsukan ke salah satu pihak [9].

Man-in-the-middle attacks didapatkan dari situasi bola di mana dua pemain bermaksud saling mengoper bola, sementara satu pemain di antara mereka mencoba merebutnya. *Man-in-the-middle attacks* berfokus pada informasi yang mengalir di antara titik akhir, kerahasiaan dan kebenaran informasi tersebut. *Man-in-the-middle attacks* adalah proses menyadap di mana dalam komunikasi antara dua perangkat A dan B, penyerang menerima A dengan berpura-pura dia adalah B. Ini berarti setiap kali A ingin mengirim pesan ke B, itu sebenarnya mengirimkannya ke penyerang yang membaca pesan kemudian meneruskannya ke B untuk membuat komunikasi tetap berfungsi. Penyerang dapat membaca semua

konten komunikasi termasuk email, gambar, dan password[9], [10]. Proses *Man-in-the-middle attacks* digambarkan pada Gbr. 1 [11].



Gbr. 1 Visualisasi *Man-in-the-middle attacks.*

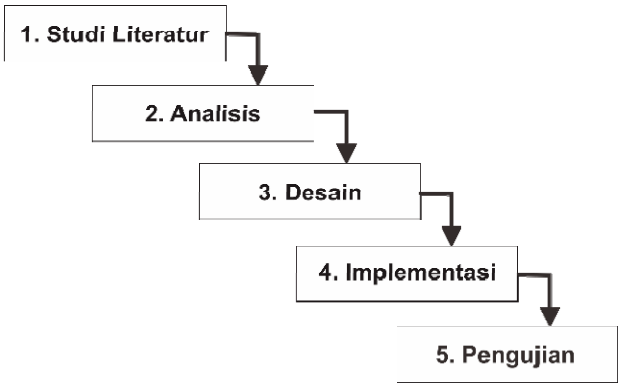
Teknologi Blockchain merupakan kumpulan beberapa konsep keamanan yang dapat digunakan untuk menjamin kerahasiaan informasi [12]. Salah satu konsep yang digunakan teknologi Blockchain seperti konsep yang digunakan pada *distributed database* [13]. Konsep *distributed database* dari teknologi Blockchain adalah dimana *database* yang terdistribusi berisi catatan transaksi yang dibagikan di antara anggota yang berpartisipasi pada *chain* tersebut. Setiap transaksi dikonfirmasi oleh konsensus mayoritas dari anggota, sehingga membuat transaksi penipuan tidak dapat terjadi. Blockchain merupakan sebuah kumpulan blok yang membentuk rantai (*chain*). Setiap blok memiliki 3 elemen yaitu data, nilai *hash* dari blok, dan nilai *previous hash* atau 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 [14], [15].

Teknologi Blockchain menyimpan data dalam bentuk *hash*, membuat data menjadi tersamarkan sehingga informasi yang terkandung dalam blok tersebut dapat tersembunyi [16]. Teknologi ini juga mampu mencegah adanya perubahan atau pemalsuan transaksi sehingga dapat digunakan untuk melakukan transaksi secara langsung secara aman. Sistem pencatatan logs yang terdistribusi dan transparan dari teknologi ini dapat menjadi solusi untuk diterapkan pada pencatatan transaksi sehingga dapat menjadi upaya untuk meminimalisir tingkat pemalsuan dan penyalahgunaan data [3].

Berdasarkan kerentanan yang diidentifikasi maka teknologi Blockchain memiliki potensi untuk dapat menanggulagi berbagai serangan. Percobaan serangan *Man-in-the-middle attacks* dapat dilakukan untuk menguji teknologi Blockchain dalam melindungi dan menjaga kerahasiaan data dari *attacker*.

II. METODOLOGI PENELITIAN

Metodologi yang digunakan pada penelitian ini merupakan metode *patching*, dimana objek yang akan diteliti sebelumnya sudah ada namun dilakukan *updating* untuk menyempurnakan objek tersebut. Adapun langkah-langkah metode *patching* dapat dilihat pada Gbr. 2.

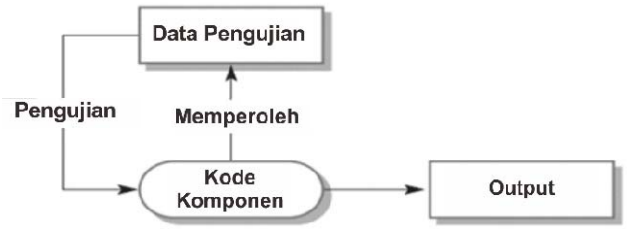


Gbr. 2 Visualisasi langkah-langkah metode *patching.*

Langkah-langkah *patching* dapat dibagi atas 5 tahapan. Tahap studi literatur, analisis, desain, implementasi dan *testing* atau pengujian yang diuraikan sebagai berikut:

1. Studi literatur, pada tahap ini dilakukan pengumpulan data baik mengenai sistem yang akan digunakan untuk penelitian, dasar teori baik mengenai *Man-in-the-middle attacks*, teori Blockchain, hingga *tools* yang akan digunakan dalam penelitian. Pengumpulan literatur terbagi atas 2 sumber, yakni dari jurnal penelitian yang berkaitan dan internet.
2. Analisis, tahap ini merupakan tahap untuk melakukan analisis kondisi saat ini mengenai sistem yang akan digunakan dalam penelitian ini, baik dari bagaimana sistem bekerja, alur sistem hingga *payload* data yang akan menjadi fokus utama pada penelitian ini. Selain itu juga percobaan *Man-in-the-middle attacks* menggunakan *tools* Burpsuite v.2020.1, sebelum diimplementasikan konsep pengamanan yang ditawarkan. Tujuan dari tahap ini adalah mendapat semua detail dari sistem yang digunakan saat ini [17].
3. Desain, hasil analisis tentu saja akan lebih jelas jika digambarkan dengan skema proses atau desain alur, sehingga pada tahap ini akan dipaparkan dan ditampilkan gambaran mengenai proses serangan dan pengamanan data yang dilakukan.
4. Implementasi, tahap ini merupakan percobaan pengimplementasian dari hasil analisis [17], kerentanan yang akan terjadi ketika sistem tersebut dianalisis akan diimplementasikan teknologi Blockchain untuk mengamankan informasi pada sistem terebut.
5. Testing, tahap ini merupakan tahap pengujian dari implementasi teknologi Blockchain yang telah dilakukan. Metode pengujian yang dilakukan adalah *White Box*

Testing seperti yang dipaparkan pada Gbr. 3 [18]. *White Box Testing* adalah metode *test case* yang sepenuhnya dikendalikan oleh pengembang [19]. *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 [20], [21]. Pengujian yang akan dilakukan adalah percobaan serangan langsung menggunakan *Man-in-the-middle attack.*



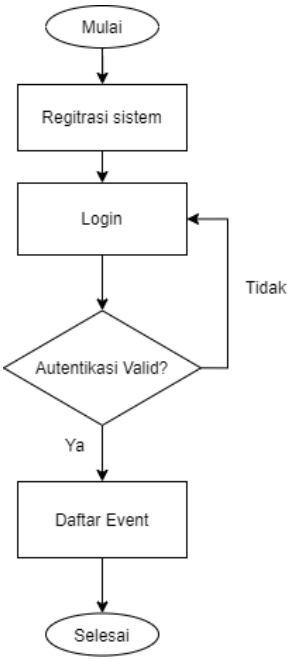
Gbr. 3 *White Box Testing.*

III. HASIL DAN PEMBAHASAN

Objek dari penelitian ini adalah proses autentikasi dari Sistem Nyebar yang digunakan oleh CV. Nyebar Inspirasi Nusantara. Sistem Nyebar merupakan aplikasi yang menjadi sebagai wadah utama untuk mengelola data-data *event*, mulai dari registrasi akun, pendaftaran event, registrasi ualng, pembayaran, hingga *feedback* dari penyelenggaraan event tersebut.

Sistem Nyebar menyediakan layanan pendaftaran akun default sebagai Member, dimana akun tersebut dapat di-*uprade* menjadi akun *Organizer* yang dapat merupakan sebuah lembaga baik profit maupun non-profit. Akun *Organizer* memiliki *privilege* untuk menyelenggarakan dan mempublikasikan event di Sistem Nyebar, mengelola data pendaftaran, dan mengelola data *feedback* dari Member, sehingga Member yang dapat mendaftarkan diri pada event-event yang tersedia.

Gbr. 4 memaparkan proses pendaftaran event seorang Member. Sebelum mendaftatr sebuah event yang ada pada Sistem Nyebar, Member harus melakukan validasi data berupa memasukkan *username* dan password atau metode lain yang digunakan untuk validasi akun. Member yang telah berhasil masuk kedalam akun dapat melakukan pendaftaran event yang di selenggarakan oleh *Organizer*



Gbr. 4 *Flowchart* Proses Pendaftaran Event.

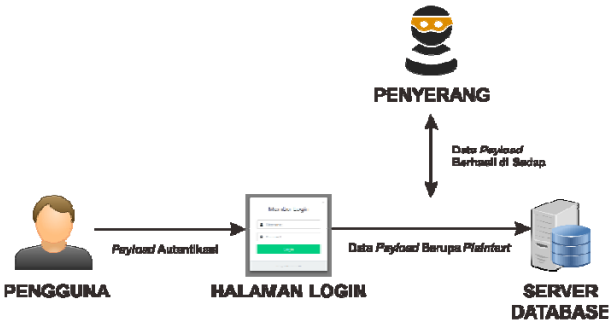
Saat ini Sistem Nyebar belum diamankan dengan baik seperti yang terlihat pada Gbr. 5. Pada Gambar tersebut terlihat bahwa *payload* data autentikasi yang dikirim masih dalam bentuk *plaintext*, sehingga data-data tersebut langsung dapat dilihat *value*-nya oleh penyerang. Data yang belum diberlakukan pengamanan yang baik dapat menyebabkan data tersebut mudah untuk disadap dan nantinya akan berdampak pada penyalahgunaan data tersebut.

Berdasarkan analisis yang dilakukan, memperoleh hasil mengenai gambaran konseptual dari proses autentikasi pada Sistem Nyebar yang dapat dilihat pada Gbr. 6. User harus melakukan autentikasi terlebih dahulu untuk mengakses Sistem Nyebar. Autentikasi yang diperlukan berupa memasukka *username* dan password dari akun yang telah terdaftar. Kondisi saat ini seperti yang telah dipaparkan pada Gbr. 5 bahwa Sistem Nyebar ketika melakukan POST data untuk autentikasi masih berupa *plaintext*, sehingga ketika dilakukan *sniffing* pada proses tersebut akan didapatkan *username* dan password yang diinputkan.

POST request to //t.co/fCUxNHP2Xh

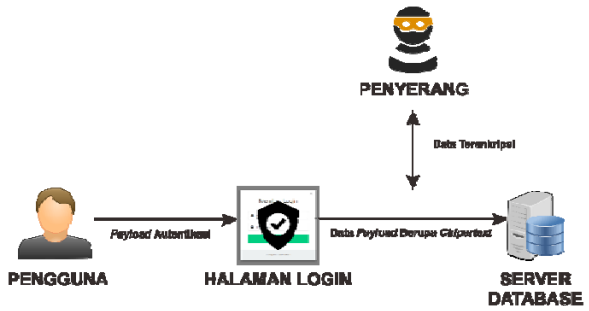
Type	Name	Value
URL	amp	1/signup
Body	email	admin
Body	password	admin

Gbr. 5 *Capture Payload* Proses Autentikasi Admin.



Gbr. 6 Konseptual Hasil Analisis Kondisi Sistem Nyebar.

Gbr. 7 memaparkan menegenai konseptual rancangan solusi keamanan dari permasalahan yang ada. Gambaran rancangan keamanan yang akan dilakukan adalah menambah *patch* pada *form* autentikasi sehingga data yang akan dikirimkan dapat diamankan, sehingga penyerang tidak dapat membaca isi *payload* data yang dikirimkan oleh pengguna.



Gbr. 7 Konseptual Rancangan Keamanan yang akan Diimplementasikan.

Teknologi Blockchain memiliki beberapa mekanisme pengamanan diantaranya pengamanan menggunakan algoritma kriptografi dengan mekanisme blok hash, *proof-of-work*, dan mekanisme penyimpanan terdistribusi [14]. Kondisi saat ini dari Sistem Nyebar adalah tidak adanya pengamanan *payload* autentikasi sehingga masih dikirimkan dalam bentuk *plaintext*, oleh karena itu mekanisme blok hash dari teknologi Blockchain memberikan peluang untuk membuat pengiriman *payload* autentikasi menjadi lebih aman.

Algoritma pembuatan blok hash dapat dilihat pada Gbr. 8. Blok hash akan dibuat ketika proses registrasi akun dan akan tersimpan dalam bentuk blok hash yang dapat digunakan untuk autentikasi user. Adapun blok hash yang akan di-*generate* berisi 0 yang merupakan *key* dari blok, *username*, dan password. *Username* adalah elemen unik sehingga dapat menanggulangi duplikasi data pada server.

```
authHash() {
   return SHA256(
      0 + this.email + this.password
   ).toString();
}
```

Gbr. 8 Algoritma Pembuatan Blok Hash.

Percobaan POST data registrasi setelah diamankan menggunakan teknogi Blockchain membuat data yang dikirimkan menjadi sebuah blok hash, sehingga data asli menjadi lebih aman dan rahasia. Data yang di POST akan disimpan ke dalam *database* server, seperti yang terlihat pada Gbr. 9.

Hasil pengujian dari *White Box Testing* dapat dilihat pada Gbr. 10. Pengujian dengan percobaan serangan *Man-in-the-middle* pada proses autentikasi menggunakan *tools* Burpsuite v.2020.1 menghasilkan *payload* data yang dikirimkan berupa blok hash atau terenkripsi, sehingga data yang terkandung dalam payload tersebut lebih terjamin keamananya dan terjaga kerahasiaanya. Gbr. 11 memaparkan status autentikasi setelah teknologi Blockchain diimplementasikan pada Sistem Nyebar.


```
{
    "status": 200,
    "result": {
        "_id": "5e70a8059b9b796073885924",
        "auth_hash": "9004e53d1304e17aa46072aa77169523660fa5c60cb2bc82f2d5aea9bc629fb7",
        "createdAt": "2020-03-17T10:35:49.121Z",
        "updatedAt": "2020-03-17T10:35:49.121Z",
        "__v": 0
    }
}
```


Gbr. 9 Data Autentikasi User yang Tersimpan di *Database*.

Gbr. 10 *Payload* Data Autentikasi User yang di *Capture* Menggunakan Burpsuite.

```
{
    "status": 200,
    "message": "Login success",
    "result": {
        "_id": "5e70a8059b9b796073885924",
        "auth_hash": "9004e53d1304e17aa46072aa77169523660fa5c60cb2bc82f2d5aea9bc629fb7",
        "createdAt": "2020-03-17T10:35:49.121Z",
        "updatedAt": "2020-03-17T10:35:49.121Z",
        "__v": 0
    }
}
```


Gbr. 11 Status Autentikasi Setelah Diimplementasikan Teknologi Blockchain.

IV. KESIMPULAN

Keamanan sistem informasi merupakan aspek yang sangat perlu untuk diperhatikan untuk menjaga data yang dikelola pada sistem tersebut. Autentikasi sebagai gerbang utama dalam sebuah sistem informasi, sehingga kerentanan-kerentanan dalam sebuah proses autentikasi harus ditanggulangi. Serangan Man-in-the-middle sebagai salah satu serangan yang dapat membuka celah kerentanan proses autentikasi. Teknologi Blockchain memiliki mekanisme blok hash yang dapat digunakan untuk menutup celah kerentanan pada proses autentikasi. Mekanisme blok hash mengubah data payload autentikasi yang berupa plaintext menjadi data chipertext dengan mengubah data tersebut menjadi blok enkripsi. Blok data tersebut tidak dapat dibaca sehingga dapat menjamin keamanan dan kerahasiaan data payload. Berdasarkan hasil yang didapatkan maka implementasi dari teknologi Blockchain berhasil mengamankan data payload autentikasi pada sebuah sistem informasi.

REFERENSI

[1] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ)," *Elinvo (Electronics, Informatics, and Vocational Education)*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[2] A. Fauzan N I, "Teknologi Blockchain dan Peranannya dalam Era Digital," *Jurnal BJB University*, vol. 4, pp. 1–15, 2018.

[3] M. D. K. Perdani, W. Widyawan, and P. I. Santosa, "Blockchain untuk Keamanan Transaksi Elektronik Perusahaan Financial Technology (Studi Kasus pada PT XYZ)," *Semnasteknomedia*, vol. 6, no. 1, pp. 7–12, 2018.

[4] F. Septa and R. Umar, "Analisis kepuasan pengguna sistem informasi e-government menggunakan metode webqual 4.0 (studi kasus: website simsarpras kementerian agama)," *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, vol. 3, no. 2, 2019.

[5] C. E. Suling, M. Olivya, and R. Nur, "Prototype Pengembangan Autentikasi Login Menggunakan Teknologi Quick Respone Code," in *Seminar Nasional Teknik Elektro dan Informatika (SNTEI) 2017*, 2017, no. November, pp. 156–161.

[6] R. Firdaus, D. Kurniawan, and E. C. Simamora, "Implementasi metode autentikasi one time password (otpa) berbasis mobile token pada aplikasi ujian online (studi kasus : jurusan matematika fmipa unila)," in *Prosiding SNSMAIP III-2012*, 2012.

[7] R. Munadi, Z. Musliyana, and T. Y. Arif, "Peningkatan Sistem Keamanan Otentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia," *Jurnal Rekayasa Elektrika*, vol. 12, no. 1, pp. 21–29, 2016.

[8] D. Saputra and I. Riadi, "Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 1, pp. 66–73, 2019, doi: 10.17781/p002558.

[9] R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, and K. M. Koumadi, "Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN)," *Journal of Computer Networks and Communications*, vol. 2019, 2019, doi: 10.1155/2019/4683982.

[10] P. Radhika, G. Ramya, K. Sadhana, and R. Salini, "Defending Man In The Middle Attacks," *International Research Journal of Engineering and Technology(IRJET)*, vol. 4, no. 3, pp. 579–585, 2017.

[11] William Stallings, *Cryptography and Network Security*, 4th ed. Prentice Hall, 2005.

[12] G. D. Putra, S. Sumaryono, and W. Widyawan, "Rancang Bangun Identity and Access Management IoT Berbasis KSI dan Permissioned Blockchain," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, vol. 7, no. 4, pp. 384–390, 2018, doi: 10.22146/jnteti.v7i4.455.

[13] Caroline Harris, "The History of Bitcoin," 2019. [Online]. Available: https://cryptocurrencynews.com/the-history-of-bitcoin/. [Accessed: 24-Feb-2020].

[14] R. C. Noorsanti, H. Yulianton, and K. Hadiono, "Blockchain - Teknologi Mata Uang Kripto (Crypto Currency)," *Prosiding SENDI_U*, vol. 3, p. 306, 2018.

[15] D. Efanov and P. Roschin, "The All-Pervasiveness of the Blockchain Technology," in *Procedia Computer Science*, 2018, pp. 116–121, doi: https://doi.org/10.1016/j.procs.2018.01.019.

[16] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys*, vol. 52, no. 3, 2019, doi: 10.1145/3316481.

[17] S. Barjtya, A. Sharma, and U. Rani, "A detailed study of Software Development Life Cycle (SDLC) Models," *International Journal Of Engineering And Computer Science ISSN*, vol. 6, no. 7, pp. 22097–22100, 2017, doi: 10.18535/ijecs/v6i7.32.

[18] Ian Sommerville, *Software Engineering, 9th Edition*, 9th ed. Scotland: University of St Andrews, 2011.

[19] Y. Irawan, "Pengujian Sistem Informasi Pengelolaan Pelatihan Kerja UPT BLK Kabupaten Kudus dengan Metode Whitebox Testing," *Sentra Penelitian Engineering dan Edukasi*, vol. 9, no. 3, pp. 59–63, 2017.

[20] S. Alfisahrin, "Pendekatan White Box Testing Untuk Menentukan Kualitas Perangkat Lunak Dengan Menggunakan Bahasa Pemrograman C++," *Paradigma*, vol. XIV, no. 1, pp. 69–78, 2012.

[21] H. B. I. Alfaris, C. Anam, and A. Masy'an, "Implementasi Black Box Testing Pada Sistem Informasi Pendaftaran Santri Berbasis Web Dengan Menggunakan PHP Dan MYSQL," *Jurnal Sains dan Teknologi*, vol. 6, no. 1, pp. 23–38, 2013.

Journal of Engineering Science and Technology
Vol. XX, No. Y (Year) PPP - QQQ

BLOCKCHAIN COULD SECURE XSS ATTACK

Abstract

Information technology has a significant impact on business aspects. An information system is one of the effects of technological advances, which become one of the means of managing information to be more effective and efficient. The use of information systems invites the vulnerability of distributed information, Cross-Site Scripting (XSS) attacks become one of the attacks that make managed data vulnerable to data manipulation which results in data being not well integrated or even unavailable. The Blockchain technology that contains information security mechanisms becomes an alternative in tackling Cross-Site Scripting (XSS) attacks. Blockchain technology converts data into blocks that are linked between one data to another using chain. Use the chainValidation() method to test the validity of the chain created. A valid chain will produce True output, and if the chain is invalid, it will give False output. False chains will be consensed with other chains that have a True value so that data consistency can be maintained. Based on that, Blockchain technology can secure data and information from Cross-Site Scripting (XSS) attacks.

Keywords: Cross-Site Scripting (XSS), Blockchain technology, chains, consensus, data consistency.

1. Introduction

Technology is developing very rapidly, making technology-laden in communication and information sharing. Technological advances play an essential role in providing data sources [1]. Information technology processes existing data into information. Information technology brings the business world more concise because technological sophistication not only cuts time but also mediates communication. As an example of such post office is no longer relevant because of communication using information networks provide faster service, so that now the post office is to function as an intermediary for the porter service rather than sending a letter [2].

The information system is an application used within an organization as a supporter of the transaction management to reporting [3]. The information system functions to make it easier to analyze data and information, thus making the task more effective and efficient [4, 5]. The need for the use of information systems (web-based) is increasingly widespread and covers various fields of life, and this has resulted in increased crime in the internet world. Security of information systems that are not goodwill cause important data and user confidentiality to be threatened [6].

Cybersecurity is an important aspect that needs to be considered in building an information system [7]. Vulnerability in an information system takes a significant risk in running a system because data and information can be misused, so the services provided are wrong and not as expected [8]. Incidence related to information security in a company, especially in financial institutions, is significant to be considered [9]. Fig. 1 is a report quoted from edgescan.com also found that high-risk vulnerabilities in information systems (web-based application) has increased significantly from 19.2 % in 2018 to 34.78 % in 2019. Vulnerability critical risk was found in External network layer systems face also more than doubled in 2019, up to 4.79 % from only 2 percent the previous year [10].

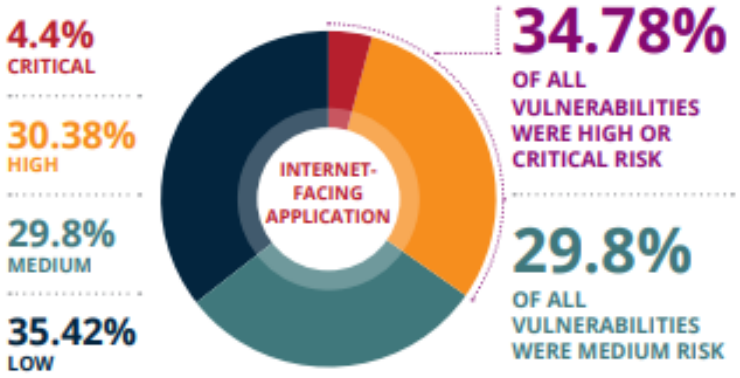


Figure 1. Percentage of high-risk vulnerabilities

The importance of securing company information is not a few that provide recommendations for making decisions about the use of third-party providers for the manufacture and operation of corporate information systems so that the system

built can be guaranteed security [11]. Security on the system information needs to be improved to tackling cyberattacks such as Cross-Site Scripting (XSS), Sniffing, and also attacks Man-in-the-middle [12].

Attacks Cross-Site Scripting (XSS) is a hacking technique that strikes a web-based system [13]. The mechanism for Cross-Site Scripting (XSS) attacks is to exploit vulnerabilities in the system by entering the script code [14]. The attacks Cross-Site Scripting (XSS) is divided into several types, including [14]:

- Session hijacking. It is like adding JavaScript that forwards cookie data to an attacker.
- Misinformation. It is like adding "For more information, contact + 62-xxx-xxx-xxx or to the notsafe.xxx page ".
- Defacing a web site. It is like adding defamation words to a web page.
- Inserting hostile content. It is like adding dangerous malware to a page.
- Phishing attacks. It is like adding fake login forms to a page.
- Takeover of the user's browser. It is like adding JavaScript code to redirect a user to another page.
- Pop-Up-Flooding. It is Malicious scripts can make a website inaccessible.

Apart from the points above, the development of Cross-Site Scripting (XSS) attacks can manipulate server resources. For example, database manipulation (input, update, delete), authentication process, and value validation [13]. This case causes data consistency to be disrupted and results in data not available and not appropriately integrated.

Blockchain technology is a collection of several security concepts that can be used to guarantee the confidentiality of information [15]. One concept used in Blockchain technology is the concept used in distributed databases [16]. The concept of distributed databases of technology Blockchain is where databases are distributed containing transaction records shared among the members participating in the chain such. Each transaction is confirmed by the consensus of the majority of members, thus making fraudulent transactions can not occur. Blockchain is a collection of blocks that make up the chain (chain). Each Block has three elements, namely data, the hash value of the Block, and the previous hash value or the hash value of the previous Block. Techniques utilizing the hash is what makes Blockchain more secure because if there is change one Block in a chain, then the value of the hash - it will change, and the next Block will be invalid because it does not save the value of hash valid from the previous Block. That is, changes made to a block will result in the entire chain being invalid [17, 18].

Blockchain technology stores data in the form of hashes, making data obscured so that the information contained in the Block can be hidden [19]. This technology is also able to prevent changes or falsification of transactions so that they can be used to make transactions directly safely. Logging systems distributed and transparency of this technology can be applied to the solution for transaction records so that it can be an attempt to minimize the level of fraud and misuse of data [20].

Based on the vulnerabilities identified, Blockchain technology has the potential to be able to respond to various attacks. The attempted attack Cross-Site Scripting (XSS) can do to test the technology Blockchain d nature to protect and maintain the confidentiality of the data of the attacker.

2. Research Methodology

This study uses an experimental method to see the effect of the object on a particular treatment being controlled [6]. The steps for the patching method can be seen in Fig. 2.

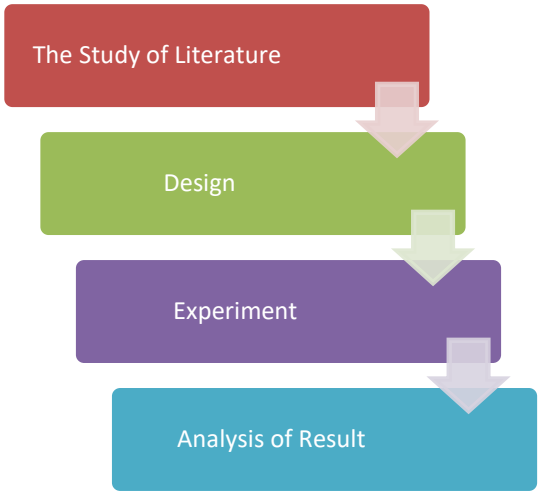


Figure 2. Visualization of the steps of the experimental method

The steps of the experiment can be divided into four stages. Stage study of literature, design design, experimentation, and analysis of the results of the test described as follows:

1. The study of literature, on this step, is done collecting data related to the fundamental basics theory about the attacks Cross-site scripting, Blockchain theory, to design implementation that will be created. The collection of literature is divided into two sources, namely from related research journals and the internet.
2. Design, the results of data collection will be more clear if described by the process or architecture scheme of the object to experiment so that at this stage will be presented and displayed a picture of the process of attack and data security carried out.
3. Experiments, at this stage, implement the results of the design made [21], the design of the XSS attack mechanism, and how the Blockchain technology detects attacks and secures them.
4. Analysis of Results, this stage is the analysis phase of the results obtained after conducting experiments. The results analysis process is carried out by testing whether the implementation of Blockchain technology successfully achieves the expected goals. The testing method used is White Box Testing, as described in Fig. 3 [22]. White Box Testing is a test case method that is fully controlled by the developer [23]. White Box Testing dramatically increases the overall effectiveness of testing, and this can more easily detect bugs that are difficult to find with Black Box Testing or other testing methods. Therefore a White Box Tester must know the programming structure [24, 25]. Testing to be carried out is a direct attack attempt using a Man-in-the-middle attack.

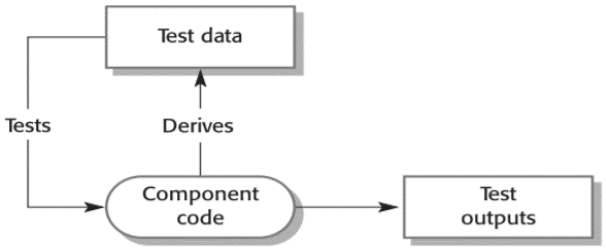


Figure 3. White Box Testing

3. Results and Discussion

Blockchain is a technology that implements Distributed Ledger Technology (DLT) or distributed bookkeeping technology, in which every participant (host) connected to a network has the privilege to access it. The concept used in the Blockchain is the same as implementing a distributed database concept [17]. The concept of Blockchain technology is the same as the concept used in distributed databases. The concept of distributed databases is that when data or information is recorded, the data will be stored and distributed to every member who is a member of the network [18].

Blockchain is a collection of more than one Block that forms a chain. Each Block has three elements, namely data, a hash value from the Block, and hash value from the previous Block. There are several mechanisms/techniques used in Blockchain so that the security of Blockchain more guaranteed [17], in an unrivaled:

1. Utilizing hash techniques, by using hash techniques from cryptography, a block will have a hash value that identifies the Block and its entire contents and is unique.
2. Mechanisms proof-of-work, This is a mechanism to slow the making of the new Block.
3. Distributed management. Blockchain uses a peer-to-peer network where everyone is allowed to join [17].

Fig. 4 describes the design of implementing the Blockchain on an information system. Blockchain is applied to secure the REST API that is sent. The REST API that is sent will be converted into an encryption block so that the data inside will be safe from eavesdropping. The Blocks made will be connected to a chain and stored in a database (nodes) that have been allowed to join to create a peer-to-peer network.

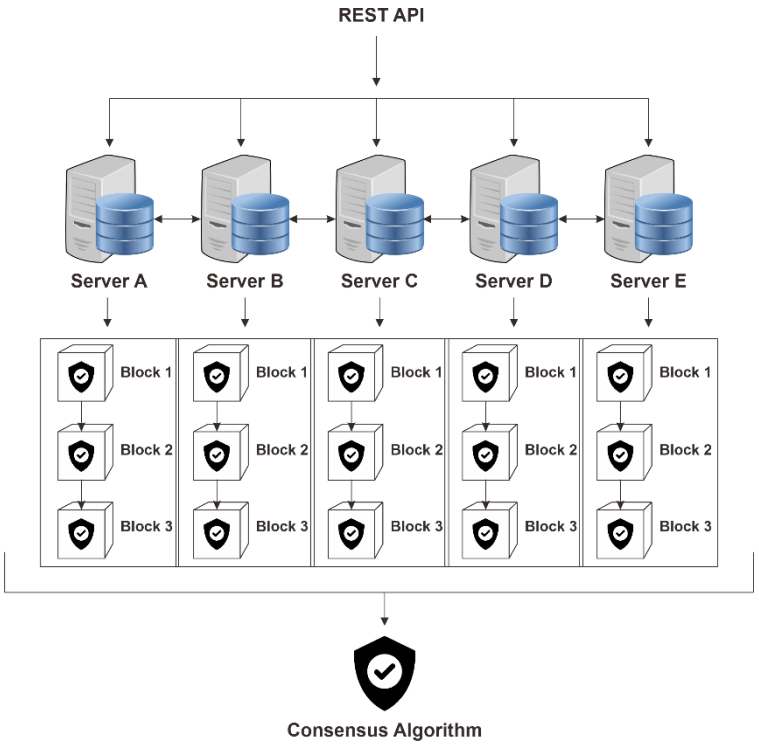


Figure 4. Design of Implementation of Blockchain in Information Systems

The Block that is created on a Blockchain contains the transaction data payload to be secured. Transaction data includes data sender, receiver, the amount submitted, the hash of the previous Block (the case of the first Block will use the genesis block), and the time the transaction took place. The data is then encrypted into a Block, and the hash of the previous Block becomes the link chain to become the Blockchain and guard the validity of the data that the data does not change. Details of the contents of the Block can be seen in Fig. 5.

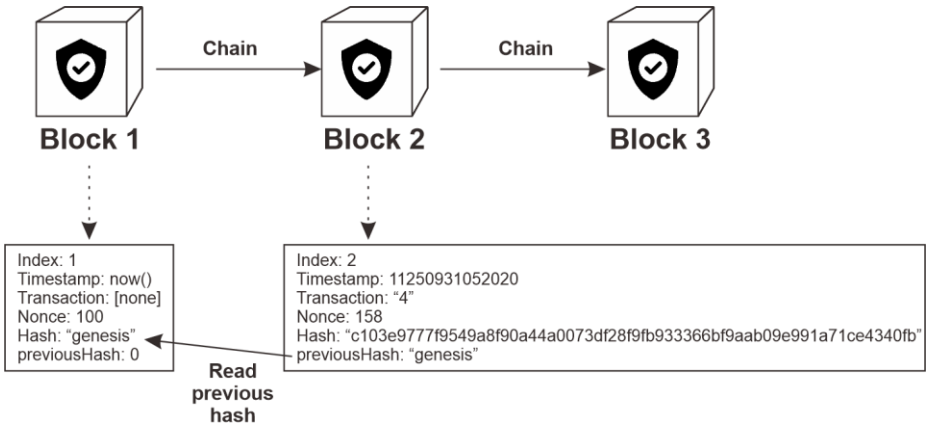


Figure 5. Data Stored in a Block

Blockchain uses a network of peer-to-peer where everyone is allowed to join. A Block which added to a node will distribute to nodes that participated in the network so that all the nodes will have a copy of the entire transaction by using a consensus mechanism. This algorithm ensures all nodes receive the same data without exception and avoids malicious actors who cheat data transactions. The way it works is only to compare the chain length of each data node. Chain valid regarded as the correct chain.

Attacks Cross-Site Scripting (XSS) is an attack injection model. This attack inserts a script that can change and even delete data on a system [13, 14, 26]. XSS attacks allow the attacker to make changes to the data, causing vulnerability to data consistency. The scenario of an XSS attack can be seen in Fig. 6, and the attempted attack data can be seen in Table 1.

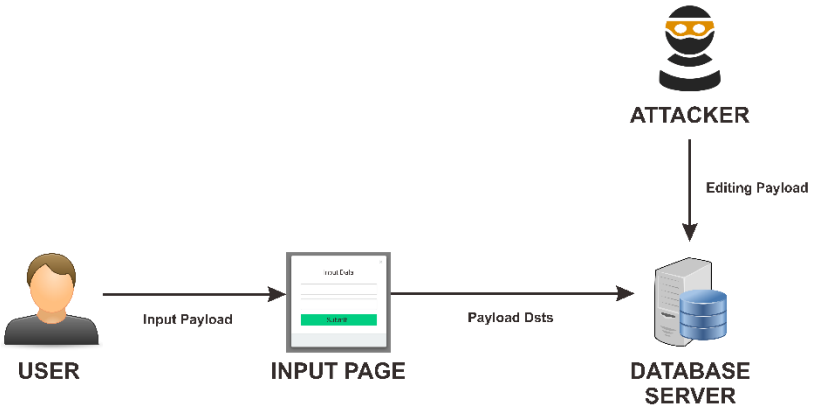


Figure 6. Data Stored in Blocks

Table 1. The experiment of Changing Block

Parameters	Block
Block Before Data Change	index: 0, data: Genesis block previous hash: 0 hash: 73c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38 index: 1, data: amount: 4 previous hash: 73c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38 hash: c103e9777f9549a8f90a44a0073df28f9fb933366bf9aab09e991a71ce4340fb index: 2, data: amount: 8 previous hash: c103e9777f9549a8f90a44a0073df28f9fb933366bf9aab09e991a71ce4340fb hash: e905c88e9684841e8a897c091a8bcecc043f37087a7f04f2b7986faaea062c81

	index: 3, data: amount: 6 previous hash: e905c88e9684841e8a897c091a8bcecc043f37087a7f04f2b7986faaea062c81 hash: d95cec7ca390e825edf593ba6ae150a872a327cb318d11367663100d7463dcce
Block After Data Change	index: 0, data: Genesis block previous hash: 0 hash: 73c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38 index: 1, data: amount: **100** previous hash: 73c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38 hash: **be58287e1b2e8762937dcc5a1f634d1738cc3f539fdd39da57058a6bc96cf5d4** index: 2, data: amount: 8 previous hash: **c103e9777f9549a8f90a44a0073df28f9fb933366bf9aab09e991a71ce4340fb** hash: e905c88e9684841e8a897c091a8bcecc043f37087a7f04f2b7986faaea062c81 index: 3, data: amount: 6 previous hash: e905c88e9684841e8a897c091a8bcecc043f37087a7f04f2b7986faaea062c81 hash: d95cec7ca390e825edf593ba6ae150a872a327cb318d11367663100d7463dcce

The scenario of an attack carried out as in Figure 6, where the user submits data, which then the data payload is sent to a database server. The attacker does edit data that cause data to change. Table 1 shows data before and after data changes.

The Blockchain technology that has a mechanism to prevent data changes and data inconsistencies can be an alternative to respond to XSS attacks. The hash mechanism that converts data into blocks and chains validates every change and or addition of blocks so that when there is an attack that damages the data in the chain, it will be detected. Distributed database mechanism becomes a solution if there is an attack that destroys data in a chain in one node by way of consensus (equalization of data) from other nodes that are trusted and valid.

The validation algorithm for a chain can be seen in Fig. 7 [27]. The chainValidation() method to test the validity of the chain created and ensured the data contained therein does not change. The algorithm will check the blocks one by one by matching the previousHash of the previous Block. A valid chain will produce True output, and if the chain is invalid, it will give False output.

```
    chainValidation() {
        for (let i = 1; i < this.chain.length; i++) {
            const currentBlock = this.chain[i];
            const previousBlock = this.chain[i - 1];
```

```
            if (currentBlock.hash !== currentBlock.calculateHash
()) {
                return false;
            }
            if (currentBlock.previousHash !== previousBlock.hash
) {
                return false;
            }
        }
        return true;
    }
```

Figure 7. Chain Validation Algorithm

Experiments carried out were experiments in making four blocks (including genesis block). One of the blocks created will be changed in value. In this case, the Block with index "1" with the data "amount" previously valued at "2" will be changed to "100"— the results of the chain validation testing experiments, as shown in Table 2. Data before being replaced produces a chain that has a True value, thus indicating that the chain is valid. While the chain where the data has been modified produce chain of value False, so it has an invalid value and needs to be changed back to valid.

Table 2. Chain Validation Results

Parameters	Blok
Block Before Data Change	index: 0, data: Genesis block previous hash: 0 hash: 73c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38 index: 1, data: amount: 4 previous hash: 73c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38 hash: c103e9777f9549a8f90a44a0073df28f9fb933366bf9aab09e991a71ce4340fb index: 2, data: amount: 8 previous hash: c103e9777f9549a8f90a44a0073df28f9fb933366bf9aab09e991a71ce4340fb hash: e905c88e9684841e8a897c091a8bcecc043f37087a7f04f2b7986faaea062c81 index: 3, data: amount: 6 previous hash: e905c88e9684841e8a897c091a8bcecc043f37087a7f04f2b7986faaea062c81 hash: d95cec7ca390e825edf593ba6ae150a872a327cb318d11367663100d7463dcce Blockchain valid? **true**

Block After Data Change	index: 0, data: Genesis block previous hash: 0 hash: 73c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38 index: 1, data: amount: **100** previous hash: 73c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38 hash: **be58287e1b2e8762937dcc5a1f634d1738cc3f539fdd39da57058a6bc96cf5d4** index: 2, data: amount: 8 previous hash: **c103e9777f9549a8f90a44a0073df28f9fb933366bf9aab09e991a71ce4340fb** hash: e905c88e9684841e8a897c091a8bcecc043f37087a7f04f2b7986faaea062c81 index: 3, data: amount: 6 previous hash: e905c88e9684841e8a897c091a8bcecc043f37087a7f04f2b7986faaea062c81 hash: d95cec7ca390e825edf593ba6ae150a872a327cb318d11367663100d7463dcce Blockchain valid? **false**
Block After Consensus	index: 0, data: Genesis block previous hash: 0 hash: 73c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38 index: 1, data: amount: 4 previous hash: 73c7fb1437035365d9228c77eca2cfd240523e274163e78c1eba11effd8b38 hash: c103e9777f9549a8f90a44a0073df28f9fb933366bf9aab09e991a71ce4340fb index: 2, data: amount: 8 previous hash: c103e9777f9549a8f90a44a0073df28f9fb933366bf9aab09e991a71ce4340fb hash: e905c88e9684841e8a897c091a8bcecc043f37087a7f04f2b7986faaea062c81 index: 3, data: amount: 6 previous hash: e905c88e9684841e8a897c091a8bcecc043f37087a7f04f2b7986faaea062c81 hash: d95cec7ca390e825edf593ba6ae150a872a327cb318d11367663100d7463dcce Blockchain valid? **true**

The consensus algorithm used to change chains that were previously False to True by matching chains in other nodes that are True. When a Chain with False value has found, each node will validate. If there is a node that has a True value, it will be used as a consensus master to make the False chain valid again. The final results of the experiments carried out can be seen in Table 3.

Table 3. The Final Result of the Experiment

No	Parameters	Before Implementation	After Implementation
1.	Editable chain	Yes	Yes
2.	Chain Validation	No	Yes
3.	Chain Consistency	No	Yes

4. Conclusions

Information security is an aspect that needs to be considered to secure data. Especially the transaction data payload that is managed in the information system. Attacks Cross-Site Scripting (XSS) is a scourge that causes endangerment consistency of payload transaction data in an information system, resulting in the integration and availability of data to be disrupted. Blockchain technology offers information security mechanisms. Using a block and chain mechanism that requires validation is a solution to check whether the transaction data payload sent continuously is True or False. Chains that are of False will be consensed with chains of value that are True so that the data will be integrated and consistent. Blockchain technology can maintain the consistency of transaction data payloads from Cross-Site Scripting (XSS) attacks

References

1. Riadi, I.; Umar, R.; and Nasrulloh, I.M. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ) [Digital Forensic Analysis on Frozen Solid State Drive with the National Institute of Justice Method (NIJ)]. *Elinvo (Electronics, Informatics, and Vocational Education)*, 3(1), 70–82.
2. Ahmad, F.N.I. (2018). Teknologi Blockchain dan Peranannya dalam Era Digital [Blockchain Technology and Its Role in the Digital Age]. *Jurnal BJB University*, 4, 1–15.
3. Septa, F.; and Umar, R. (2019). Analisis Kepuasan Pengguna Sistem Informasi E-Government Menggunakan Metode Webqual 4.0 (Studi Kasus: Website Simsarpras Kementerian Agama) [E-Government Information System User Satisfaction Analysis Using Webqual 4.0 Method (Case Study: Ministry of Religion Simsarpras Website)]. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, 3(2), 127-135.
4. Komalasari, N.; Murad, D.F.; Agustine, D.; Irsan, M.; Budiman, J.; and Fernando, E. (2018). Effect of education, performance, position and information technology competency of information systems to performance of information system. *2018 International Seminar on Research of Information Technology and Intelligent Systems*. 221–226.

5. Xue, G.; Wu, Y.; and Xu, Y. (2019). Information Enterprise Architecture for Smart Transportation System. *2019 IEEE 8th Data Driven Control and Learning Systems Conference (DDCLS)*. 1055–1059.
6. Yulianingsih, Y. (2017). Melindungi Aplikasi dari Serangan Cross Site Scripting dengan Metode Metacharacter [Protecting Applications from Cross Site Scripting Attacks with the Metacharacter Method]. *Jurnal Nasional Teknologi dan Sistem Informasi*, 3(1), 83–88.
7. Firdaus, R.; Kurniawan, D.; and Simamora, E.C. (2012). Implementasi Metode Autentikasi One Time Password (OTPA) Berbasis Mobile Token pada Aplikasi Ujian Online (Studi Kasus: Jurusan Matematika FMIPA UNILA) [Implementing Token-Based One Time Password (OTPA) Authentication Method in Online Examination Application (Case Study: Department of Mathematics, FMIPA UNILA)]. *Proceeding SNSMAIP III-2012*. 60–67.
8. Dobrovoljc, A.; Trček, D.; and Likar, B. (2017). Predicting exploitations of information systems vulnerabilities through attackers' characteristics. *IEEE Access*, 5(10), 26063–26075.
9. Astakhova, L.; and Muravyov, N. (2019). A Data Collection and Analysis System for Managing the Vulnerabilities of Users of an Information System in a Small Business. *Proceedings - 2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology*, 193–196.
10. Anonymous. (2020). Edgescan's 2020 Vulnerability Stats Report Released. Retrieved May 30, 2020, from https://www.edgescan.com/edgescans-2020-vulnerability-stats-report-released/.
11. Kozlov, A.D.; and Noga, N.L. (2018). Risk Management for Information Security of Corporate Information Systems Using Cloud Technology. *Proceedings of 2018 11th International Conference & Management of Large-Scale System Development*. 1–5.
12. Saputra, D.; and Riadi, I. (2019). Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method. *International Journal of Cyber-Security and Digital Forensics*, 8(1), 66–73.
13. Jayantha, M.D.; Dharma, E.M.; and Firdaus, Y. (2007). Analisis tingkat kemanan terhadap cross-site scripting pada aplikasi web berbasis ajax dibandingkan dengan aplikasi web konvensional [Security level analysis of cross-site scripting in ajax-based web applications compared to conventional web applications]. *Telkom University*, 1–6.
14. Nithya, V.; Pandian, S.L.; and Malarvizhi, C. (2015). A survey on detection and prevention of cross-site scripting attack. *International Journal of Security and its Applications*, 9(3), 139–152.
15. Putra, G.D.; Sumaryono, S.; and Widyawan, W. (2018). Rancang Bangun Identity and Access Management IoT Berbasis KSI dan Permissioned Blockchain [Design of Identity and Access Management IoT Based KSI and Permissioned Blockchain]. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, 7(4), 384–390.
16. Harris, C. (2019). The History of Bitcoin. Retrieved February 24, 2020, from https://cryptocurrencynews.com/the-history-of-bitcoin/.

17. Noorsanti, R.C.; Yulianton, H.; and Hadiono, K. (2018). Blockchain - Teknologi Mata Uang Kripto (Crypto Currency) [Blockchain - Crypto Currency Technology]. *Prosiding SENDI_U*, 1–6.
18. Efanov, D.; and Roschin, P. (2018). The All-Pervasiveness of the Blockchain Technology. *Procedia Computer Science*, 116–121.
19. Zhang, R.; Xue, R.; and Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys*, 52(3), 51–85.
20. Perdani, M.D.K.; Widyawan, W.; and Santosa, P.I. (2018). Blockchain untuk Keamanan Transaksi Elektronik Perusahaan Financial Technology (Studi Kasus pada PT XYZ) [Blockchain for the security of Electronic Technology Company Electronic Transactions (Case Study at PT XYZ)], *Semnasteknomedia*, 6(1), 7–12.
21. Barjtya, S.; Sharma, A.; and Rani, U. (2017). A detailed study of Software Development Life Cycle (SDLC) Models. *International Journal Of Engineering And Computer Science*, 6(7), 22097–22100.
22. Sommerville, I. (2011). *Software Engineering* (9th ed.). Scotland: University of St Andrews.
23. Irawan, Y. (2017). Pengujian Sistem Informasi Pengelolaan Pelatihan Kerja UPT BLK Kabupaten Kudus dengan Metode Whitebox Testing [Testing the Management Information System of UPT BLK Job Training in Kudus Regency using the Whitebox Testing Method]. *Sentra Penelitian Engineering dan Edukasi*, 9(3), 59–63.
24. Alfisahrin, S. (2012). Pendekatan White Box Testing Untuk Menentukan Kualitas Perangkat Lunak Dengan Menggunakan Bahasa Pemrograman C++ [White Box Testing Approach To Determine Software Quality Using the C ++ Programming Language]. *Paradigma*, 14(1), 69–78.
25. Alfaris, H.B.I.; Anam, C.; and Masy'an, A. (2013). Implementasi Black Box Testing Pada Sistem Informasi Pendaftaran Santri Berbasis Web Dengan Menggunakan PHP Dan MYSQL [Black Box Testing Implementation on Web-Based Santri Registration Information System Using PHP and MYSQL]. *Jurnal Sains dan Teknologi*, 6(1), 23–38.
26. KirstenS. (2020). Cross Site Scripting (XSS). Retrieved May 6, 2020, from https://owasp.org/www-community/attacks/xss/.
27. Savjee. (2017). Writing a tiny blockchain in JavaScript. Retrieved May 7, 2020, from Available: https://www.savjee.be/2017/07/Writing-tiny-blockchain-in-JavaScript/.