Pengamanan Integritas Alamat Bitcoin Karyawan menggunakan Algoritma MD5

Diajukan Untuk Menyusun Skripsi di Jurusan Teknik Informatika Fakultas Ilmu Komputer UNSRI

Oleh:

Rendy Wijaya

NIM: 09021381621094

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2020

LEMBAR PENGESAHAN TUGAS AKHIR

PENGAMANAN INTEGRITAS ALAMAT BITCOIN KARYAWAN MENGGUNAKAN ALGORITMA MD5

Oleh:

RENDY WIJAYA
NIM : 09021381621094

Palembang, Juni 2020

Pembimbing I,

Drs. Megah Mulya, M.T
NIP. 196602202006041001

Pembimbing II,

Mastura Diana Marieska, S.T., M.T
NIP. 198603212018032001

Mengetahui,
Ketua Jurusan Teknik Informatika,

Rifkie Primartha, MT
NIP. 197706012009121004

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Selasa tanggal 12 Mei 2020 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Rendy Wijaya
NIM : 09021381621094
Judul : Pengamanan Integritas Alamat Bitcoin Karyawan Menggunakan Algoritma MD5.

1. Pembimbing I

   Drs. Megah Mulya, M.T
   NIP. 196602202006041001 .....

2. Pembimbing II

   Mastura Diana Marieska, S.T., M.T
   NIP. 198603212018032001 .....

3. Penguji I

   Hardini Novianti, M.T
   NIP. 197911012014042002 .....

4. Penguji II

   Danny Matthew Saputra, M.Cs
   NIP. 198503102015041002 .....

Mengetahui,
Ketua Jurusan Teknik Informatika

Rifkie Primartha, MT
NIP. 197706012009121004

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Rendy Wijaya
NIM	: 09021381621094
Program Studi	: Teknik Informatika
Judul Skripsi	: Pengamanan Integritas Alamat Bitcoin Karyawan Menggunakan Algoritma MD5.
Hasil Pengecekan Software *iThenticate/Turnitin*	: 10%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, Juni 2020

Rendy Wijaya
NIM. 09021381621094

MOTTO DAN PERSEMBAHAN

“One day or day one, you decide”

“The future belongs to those who believe in the beauty of their dreams”

- Eleanor Roosevelt-

Kupersembahkan karya tulis ini kepada :

- **Orangtuaku dan adikku tercinta**
- **Keluarga dan kerabatku**
- **Sahabat-sahabat seperjuangan**
- **Fakultas Ilmu Komputer**
- **Universitas Sriwijaya**

ABSTRACT

The focus of this research is securing the integrity and authentication of employee bitcoin addresses using the MD5 algorithm (Message Digest 5). Research carried out is developing employee payroll applications using bitcoin which is also equipped with security integrity and employee bitcoin address authentication. Application development in this study uses the API (Application Programming Interface) that has been provided by Indodax and used to pay employees using Bitcoin. Integrity security is carried out after the employee's personal data, one of which contains the bitcoin address is stored in the database, which will then generate the hash value of the bitcoin address using the MD5 algorithm and stored in a separate database. Bitcoin address authentication is done when will payroll using bitcoin, the process that is done is to generate the bitcoin address hash value stored in the database using the MD5 algorithm and compare the hash value with the hash value that has been stored in a separate database before. Based on testing that has been done, the MD5 algorithm can be used to ensure the integrity of bitcoin addresses and detect if there is a change in bitcoin addresses with an average integrity security time of 133.64 ms and an average authentication time of 134.84 ms.

Keywords: MD5 (Message Digest 5), API (Application Programming Interface)

ABSTRAK

Fokus penelitian ini adalah pengamanan integritas dan otentikasi alamat bitcoin karyawan dengan menggunakan algoritma MD5 (*Message Digest 5*). Penelitian yang dilakukan yaitu mengembangkan aplikasi penggajian karyawan dengan menggunakan bitcoin yang juga dilengkapi dengan pengamanan integritas dan otentikasi alamat bitcoin karyawan. Pengembangan aplikasi pada penelitian ini menggunakan API (*Application Programming Interface*) yang telah disediakan oleh Indodax dan digunakan untuk melakukan penggajian karyawan menggunakan bitcoin. Pengamanan integritas dilakukan setelah data pribadi karyawan yang salah satunya berisi alamat bitcoin disimpan di dalam basis data, yang kemudian akan dilakukan pembangkitan nilai *hash* terhadap alamat bitcoin tersebut menggunakan algoritma MD5 dan disimpan di dalam basis data terpisah. Otentikasi alamat bitcoin dilakukan pada saat akan melakukan penggajian menggunakan bitcoin, proses yang dilakukan yaitu membangkitkan nilai *hash* alamat bitcoin yang tersimpan di dalam basis data menggunakan algoritma MD5 dan membandingkan nilai *hash* tersebut dengan nilai *hash* yang telah disimpan pada basis data terpisah sebelumnya. Berdasarkan pengujian yang telah dilakukan, algoritma MD5 dapat digunakan untuk menjamin integritas alamat bitcoin dan mendeteksi jika terjadi perubahan alamat bitcoin dengan rata-rata waktu pengamanan integritas sebesar 133.64 ms dan rata-rata waktu otentikasi sebesar 134.84 ms.

Kata Kunci: MD5 (*Message Digest 5*), API (*Application Programming Interface*)

KATA PENGANTAR

Penulis ucapkan puji syukur kepada Tuhan Yang Maha Esa karena penulis dapat menyelesaikan Tugas Akhir dengan judul **"Pengamanan Integritas Alamat Bitcoin Karyawan Menggunakan Algoritma MD5"** dengan baik untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin mengucapkan terimakasih kepada pihak-pihak yang telah berperan memberikan bantuan dan dukungan baik secara langsung maupun secara tidak langsung dalam menyelesaikan tugas akhir ini. Penulis ingin menyampaikan rasa terima kasih kepada:

1. Kedua orang tuaku, Wijaya Kesuma Jap dan Jenny, adikku, Ricky Wijaya serta seluruh keluarga dan kerabatku, yang selalu memberikan dukungan dan mendoakanku untuk selalu menjadi lebih baik lagi.
2. Bapak Jaidan Jauhari, M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya beserta jajarannya. Bapak Rifkie Primartha selaku Ketua Jurusan Teknik Informatika beserta jajarannya, dan Ibu Alvi Syahrini Utami selaku Sekretaris Jurusan Teknik Informatika.
3. Bapak Drs. Megah Mulya, M.T selaku dosen pembimbing I dan Ibu Mastura Diana Marieska, S.T., M.T selaku pembimbing II yang telah membimbing, mengarahkan, dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
4. Bapak M. Fachrurrozi, S.Si., M.T. selaku dosen pembimbing akademik, yang telah membimbing, mengarahkan dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
5. Ibu Hardini Novianti, MT selaku dosen penguji I, dan Bapak Danny Matthew Saputra, M.Cs selaku dosen penguji II yang telah memberikan masukan dan dorongan dalam proses pengerjaan Tugas Akhir.

6. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Pak Tony, Mbak Anna dan Mbak Wiwin beserta seluruh staf tata usaha yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.
8. Sahabat-sahabat seperjuangan dalam hidupku yang selalu memberikan dukungan baik itu dalam suka maupun duka, yang selalu membantu dalam kondisi apapun.
9. Teman-teman jurusan Teknik Informatika yang telah berbagi keluh kesah, motivasi, semangat, dan canda tawa selama masa perkuliahan.
10. Seluruh pihak yang telah membantu dalam penyusunan dan penyempurnaan tugas akhir ini yang tidak dapat disebutkan satu persatu.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan disebabkan keterbatasan pengetahuan dan pengalaman, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Tugas Akhir ini dapat berguna dan bermanfaat bagi kita semua.

Palembang, Juni 2020

Rendy Wijaya

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I

LATAR BELAKANG

1.1 Pendahuluan

Pada bab ini akan berisikan penjelasan mengenai latar belakang pengambilan topik “Pengamanan Integritas Alamat Bitcoin Karyawan menggunakan Algoritma MD5” sebagai bahan penelitian. Pada bab ini juga akan menjelaskan rumusan masalah, tujuan serta manfaat penelitian, batasan masalah dan sistematika penulisan.

1.2 Latar Belakang

Pada era sekarang tidak dipungkiri bahwa uang merupakan alat pembayaran yang sah. Pada jaman dahulu sebelum adanya uang orang-orang melakukan barter atau kegiatan tukar-menukar barang untuk mendapatkan barang yang mereka inginkan. Hingga saat ini mungkin masih ada sebagian orang yang melakukan transaksi dengan cara barter atau bisa juga melakukan tukar-menukar dengan cara tukar tambah.

Dengan kemajuan teknologi perkembangan uang sebagai alat pembayaran semakin pesat. Adanya suatu sistem perbankan untuk menyimpan uang agar lebih aman. Pembayaran dengan uang juga sudah tidak selalu menggunakan uang fisik saja, karena dengan kemajuan teknologi pembayaran bisa dilakukan dengan menggunakan kartu debit atau kartu kredit yang memiliki saldo uang yang sesuai dengan barang yang dibeli.

Perkembangan uang tidak hanya sampai tahap ini saja, kini telah diperkenalkan adanya mata uang digital atau *cryptocurrency*. Mata uang digital

sekarang sedang berkembang begitu cepat dan agresif. Menurut (Kaushal, Bagga, & Sobti, 2017) konsep *cryptocurrency* bukan merupakan hal baru, *cryptocurrency* pertama kali diperkenalkan oleh Wei Dai pada tahun 1928. Salah satu *cryptocurrency* yang paling populer saat ini adalah bitcoin.

Pada tahun 2009 seorang *hacker* dengan nama samaran Satoshi Nakamoto membuat jaringan *peer-to-peer* untuk sebuah sistem keuangan yang terdesentralisasi yang disebut bitcoin. Bitcoin diciptakan untuk menyediakan tempat peredaran uang tanpa adanya sekumpulan orang atau lembaga yang mengontrol (Kaushal et al., 2017). Dalam hal ini, sistem keuangan bitcoin memiliki daya tarik tersendiri bagi penggunanya. Basis dari bitcoin yaitu teknologi *blockchain*. Beberapa pihak pernah mengklaim kalau hampir tidak mungkin untuk membobol keamanan *blockchain*. Hal ini dapat meningkatkan kepercayaan orang-orang untuk menggunakan bitcoin, mengingat teknologi *blockchain* ini seiring berjalannya waktu semakin banyak yang menggunakan karena sudah diakui keamanannya.

Bitcoin dilengkapi dengan fitur keamanan algoritma *SHA-256* dan *Eliptic Curve* yang berfungsi untuk membangkitkan alamat bitcoin dan mengamankan transaksi bitcoin yang tercatat dalam *blockchain*. Pengguna bitcoin di Indonesia juga terus meningkat seiring berjalannya waktu, apalagi karena bitcoin dan *cryptocurrency* sudah ditetapkan secara resmi oleh Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) sebagai subjek komoditi yang dapat diperdagangkan di bursa perdagangan berjangka. Hingga saat ini bitcoin sering digunakan untuk jual beli berbagai macam *cryptocurrency*, investasi jangka

panjang dan juga sudah digunakan sebagai alat pembayaran yang sah di berbagai negara-negara maju. Salah satunya adalah negara Jepang yang juga telah menerapkan sistem penggajian karyawannya dengan menggunakan Bitcoin[1)]. Sehingga tidak menutup kemungkinan untuk kedepannya khususnya di Indonesia juga menerapkan sistem penggajian karyawannya dengan menggunakan Bitcoin, apalagi melihat minat masyarakat Indonesia untuk menggunakan bitcoin semakin meningkat.

Melakukan transaksi bitcoin berarti sudah menyetujui aturan penggunaan bitcoin. Salah satu aturan yang harus diperhatikan yaitu bahwa segala transaksi bitcoin yang terjadi dan sudah masuk ke dalam *blockchain* tidak bisa dibatalkan. Kesalahan yang sangat fatal apabila bitcoin terkirim ke alamat yang bukan seharusnya, karena dapat dianggap bahwa bitcoin tersebut hilang selamanya. Dengan mengembangkan suatu sistem penggajian karyawan menggunakan bitcoin, dibutuhkan suatu prosedur pengamanan untuk mencegah kesalahan transaksi dengan melakukan otentikasi terhadap integritas alamat bitcoin yang dituju. Pada penelitian ini alamat bitcoin yang dituju merupakan alamat bitcoin karyawan yang digunakan untuk menerima gaji bulanan.

Salah satu algoritma yang dapat digunakan untuk menjamin integritas dan proses otentikasi yaitu algoritma MD5. Algoritma MD5 dianggap tepat untuk kasus ini karena algoritma ini mempunyai kecepatan yang dapat diandalkan dalam melakukan proses *hash* yang dibutuhkan saat melakukan proses otentikasi dan pernah diterapkan oleh (Sundar, Kishore, & Suresh, 2018) untuk menjamin

---

1) Artikel berita “Tribunnews”,26 Desember 2017

integritas data hasil *e-voting.* Kelebihan lain algoritma MD5 adalah sangat kecil kemungkinan untuk terjadi *hash collision.*

1.3 Perumusan Masalah

Berdasarkan latar belakang di atas, permasalahan yang timbul adalah bagaimana penerapan algoritma MD5 (*Message Diggest 5)* dalam menjamin integritas dan melakukan otentikasi alamat bitcoin karyawan.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah

1. Mengembangkan suatu skema pengamanan untuk menjamin integritas alamat bitcoin karyawan.
2. Mengembangkan suatu skema penggajian karyawan dengan menggunakan bitcoin yang dilengkapi dengan otentikasi alamat bitcoin karyawan.
3. Mengembangkan suatu aplikasi penggajian karyawan menggunakan bitcoin dengan fitur otentikasi untuk menjamin integritas alamat bitcoin karyawan menggunakan algoritma MD5.
4. Menguji skema yang telah dibuat dengan menggunakan kasus uji coba.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah

1. Mengamankan integritas data yang berupa alamat bitcoin karyawan.
2. Menciptakan inovasi media alternatif dalam sistem gaji karyawan.

1.6 Batasan Masalah

Dalam pembuatan aplikasi penggajian karyawan dengan bitcoin, untuk mengatasi permasalahan yang ada maka penyusun membatasi permasalahan sebagai berikut :

1. API (*Application Programming Interface*) bitcoin e*xchange* yang digunakan adalah milik indodax, karena indodax merupakan salah satu bitcoin *exchange* terpercaya yang memberikan akses API untuk para *programmer* dan memiliki anggota terbanyak di Indonesia. API yang digunakan adalah *public* API dan *private* API.
2. Akun bitcoin yang dipakai berasal dari indodax dan *blockchain*.
3. Proses otentikasi hanya terjadi pada saat melakukan penggajian karyawan.
4. Aplikasi yang dikembangkan harus dalam kondisi terhubung dengan internet saat pemakaian.

1.7 Sistematika Penulisan

Sistematika Penulisan penelitian ini akan disusun dengan rangkaian sebagai berikut:

BAB I Pendahuluan

Pada bab ini akan dijelaskan mengenai latar belakang, rumusan masalah, tujuan, manfaat, batasan penelitian dan sistematika penelitian.

BAB II Tinjauan Pustaka

Pada bab ini akan dijelaskan dasar-dasar teori yang digunakan dalam penelitian seperti *blockchain*, *cryptocurrency*, bitcoin, kriptografi, tujuan

kriptografi, komponen pada kriptografi, jenis kriptografi, fungsi *hash*, otentikasi dan MD5 (*Message Digest 5*).

BAB III Analisis dan Perancangan

Pada bab ini akan dijelaskan data yang akan digunakan pada penelitian, cara mengumpulkan data tersebut, tahapan penelitian yang akan diimplementasikan, metode pengembangan perangkat lunak serta manajemen proyek penelitian.

1.8 Kesimpulan

Pada bab ini telah dijelaskan latar belakang permasalahan yang akan diselesaikan yaitu, mengenai pengamanan integritas alamat bitcoin karyawan. Perangkat lunak yang dikembangkan dapat digunakan untuk melakukan penggajian karyawan dengan bitcoin yang dilengkapi dengan fitur otentikasi untuk menjamin integritas alamat bitcoin karyawan dengan menggunakan algoritma MD5.

DAFTAR PUSTAKA

Kaushal, P. K., Bagga, A., & Sobti, R. (2017). Evolution of bitcoin and security risk in bitcoin wallets. *2017 International Conference on Computer, Communications and Electronics, COMPTELIX 2017*, 172–177. https://doi.org/10.1109/COMPTELIX.2017.8003959

Sundar, N. A., Kishore, M. V, & Suresh, P. C. (2018). A Secure E-Voting System Using RSA and Md5 Algorithms Using Random Number Generators, *13*(11), 9468–9473.

Akram, W. (2018). BLOCKCHAIN TECHNOLOGY : CHALLENGES AND FUTURE PROSPECTS Available Online at www.ijarcs.info BLOCKCHAIN TECHNOLOGY : CHALLENGES AND FUTURE PROSPECTS, *8*(September 2017), 6–9. https://doi.org/10.26483/ijarcs.v8i9.4950

B Sasi, S. (2014). A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security. *IOSR Journal of Engineering*, *4*(3), 01–04. https://doi.org/10.9790/3021-04330104

Maliberan, E. V., Sison, A. M., & Medina, R. P. (2018). A new approach in expanding the hash size of MD5. *International Journal of Communication Networks and Information Security*, *10*(2), 374–379.

Mishra, S., Mishra, S., & Kumar, N. (2013). Hashing Algorithm : MD5, *1*(9),

931–933.

Alam Hossain, M. (2012). Cryptanalyzing of Message Digest Algorithms MD4 and MD5. *International Journal on Cryptography and Information Security*, *2*(1), 1–13. https://doi.org/10.5121/ijcis.2012.2101

Rahouti, M., Xiong, K., & Ghani, N. (2018). Bitcoin Concepts, Threats, and Machine-Learning Security Solutions. *IEEE Access*, *6*(c), 67189–67205. https://doi.org/10.1109/ACCESS.2018.2874539

Spithoven, A. (2019). Theory and Reality of Cryptocurrency Governance. *Journal of Economic Issues*, *53*(2), 385–393. https://doi.org/10.1080/00213624.2019.1594518

Srivastav, S., & Verma, N. (2015). Improving Data Security in Cloud Computing Using RSA Algorithm and MD5 Algorithm, 5450–5457. https://doi.org/10.15680/IJIRSET.2015.0407084

Tripathi, R., & Agrawal, S. (2014). Comparative Study of Symmetric and Asymmetric Cryptography. *International Journal of Advance Foundation and Research in Computer*, *1*(6), 68–76. Retrieved from https://pdfs.semanticscholar.org/e0e4/810c5276f9c05cc82425fcf911f206c52bef.pdf