Pengamanan Integritas dan Otentikasi Data Pelanggan pada Sistem PT. Pos Indonesia menggunakan Algoritma MD5

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

Oleh:

Syahrul Ramadhan Aryadita Sutarno

NIM: 09021381621100

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2020

LEMBAR PENGESAHAN TUGAS AKHIR

PENGAMANAN INTEGRITAS DAN OTENTIKASI DATA PELANGGAN PADA SISTEM PT. POS INDONESIA MENGGUNAKAN ALGORITMA MD5

Oleh:

SYAHRUL RAMADHAN ARYADITA SUTARNO
NIM : 09021381621100

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 : Syahrul Ramadhan Aryadita Sutarno
NIM : 09021381621100
Judul : Pengamanan Integritas dan Otentikasi Data Pelanggan pada Sistem PT. Pos Indonesia 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. 198505102015041002

Mengetahui,
Ketua Jurusan Teknik Informatika

Rifkie Primartha, MT
NIP. 197706012009121004

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Syahrul Ramadhan Aryadita Sutarno
NIM	: 09021381621100
Program Studi	: Teknik Informatika
Judul Skripsi	: Pengamanan Integritas Dan Otentikasi Data Pelanggan Pada Sistem Pt. Pos Indonesia Menggunakan Algoritma MD5.
Hasil Pengecekan Software *iThenticate/Turnitin*	: 19%

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

Syahrul Ramadhan Aryadita Sutarno
NIM. 09021381621100

MOTTO DAN PERSEMBAHAN

“Everything (That Happens) is By Way of AL-QADR, Even You Place Your Hand Upon Your Cheek”

-IBN ABBAS-

凡事感激

Kupersembahkan karya tulis ini kepada :

- **Orangtuaku dan saudaraku tercinta**
- **Keluarga besarku**
- **Sahabat-sahabat seperjuangan**
- **Fakultas Ilmu Komputer**
- **Universitas Sriwijaya**

ABSTRACT

The focus of this research which in collaboration with PT.Pos Indonesia is securing the integrity and guaranteeing the authenticity (authentication) of customer data contained in a RFID-based (Radio Frequency Identification) customer card using MD5 algorithm (Message Digest 5). Study was done by using "Multi Client Service Registration Software" software module own by PT.Pos Indonesia as the main module, that added some process to securing customer's data integration and for authentication of customer's data according with RFID-based customer card. The process of securing customer data integration was done at the time of customer registration occurred, where the customer data index which of: NIK, customer number, and the hash value of customer's data will be inserted into the database as a reference for the authentication process. For the authentication process will occur during the service registration process, the process includes reading all of the customer's data based on the RFID card and generate the hash value using the MD5 algorithm, and compare the generated hash value with the hash value that stored in the database. Based on the test, MD5 algorithm can ensure data integrity and detect change in customer's data on RFID-based card with average time for securing data integrity is 2,041ms, and average time for the authentication process time is 150.91ms.

Keywords: MD5 (Message Digest 5), RFID (Radio Frequency Identifitcation)

ABSTRAK

Fokus penelitian yang berkerjasama dengan PT.Pos Indonesia ini adalah pengamanan integritas dan penjaminan integritas (otentikasi) data pelanggan yang terdapat pada kartu pelanggan berbasis kartu RFID (*Radio Frequency Identification*) dengan menggunakan algoritma MD5 (*Message Digest 5*). Penelitian dilaksanakan dengan menggunakan modul perangkat lunak "Aplikasi pendaftaran layanan berbasis multi client" milik PT.Pos Indonesia sebagai modul utama yang kemudian ditambahkan proses pengamanan integritas data pelanggan dan proses otentikasi terhadap keaslian data pelanggan yang berada pada kartu RFID. Pengamanan integritas data pelanggan dilakukan pada saat pendaftaran pelanggan dimana indeks data pelanggan berupa NIK, nomor pelanggan, dan nilai hash data pelanggan akan dimasukkan kedalam basis data sebagai acuan proses otentikasi. Otentikasi data dilakukan saat pendaftaran layanan yang meliputi pembacaan keseluruhan data pelanggan pada kartu RFID, pembangkitkan nilai *hash* menggunakan algoritma MD5 berdasarkan data yang dibaca, dan membandingkan nilai *hash* yang dibangkitkan dengan nilai hash yang tersimpan pada basis data. Berdasarkan pengujian yang dilakukan, algoritma MD5 dapat menjamin integritas data dan mendeteksi adanya perubahan data pelanggan pada kartu RFID dengan rata—rata waktu pengamanan integritas sebesar 2.041*ms*, dan rata—rata waktu proses otentikasi sebesar 150,91*ms.*

Kata Kunci: MD5 *(Message Digest 5)*, RFID *(Radio Frequency Identifitcation)*

KATA PENGANTAR

Penulis ucapkan puji syukur kepada Allah atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir dengan judul **"Pengamanan Integritas dan Otentikasi Data Pelanggan pada Sistem PT. Pos Indonesia 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, Sutarno dan Syamsiah, saudaraku, Syanno Revy Aryadita Sutarno, Dimas Agung Habibullah Aryadita Sutarno dan seluruh keluarga besarku, yang selalu mendokan serta memberikan dukungan baik moril maupun materil.
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. Ibu Mastura Diana Marieska, S.T., 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 terbaik dalam hidupku yang selalu memberikan *support.*
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

Syahrul Ramadhan Aryadita Sutarno

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I
PENDAHULUAN

1.1 Pendahuluan

Pada bab ini akan dijelaskan mengenai latar belakang diambilnya topik "Pengamanan Integritas dan Otentikasi data Pelanggan pada Sistem PT. Pos Indonesia menggunakan Algoritma MD5" sebagai bahan penelitian. Pada bab ini juga tercakup tujuan penelitian, manfaat penelitian yang akan dilaksanakan dan Batasan masalah dari penelitian yang akan dilaksanakan.

1.2 Latar Belakang

Perusahaan pengiriman barang pada era modern tentunya memiliki peranan penting, baik dalam perkembangan ekonomi modern maupun peredaran barang—barang logistik di berbagai daerah. Dengan menggunakan perusahaan pengiriman, peredaran barang—barang ke berbagai daerah tentunya akan menjadi lebih mudah, akan tetapi dengan hadirnya perusahaan jasa pengiriman barang juga membuka celah bagi para oknum criminal untuk melakukan tindak kejahatan. Pada tahun 2017 terjadi kasus pengedaran narkotika jenis sabu di Indonesia melalui jalur pengiriman ekspedisi kargo REX[1)]. Skema pengiriman barang yang dilakukan oleh pelaku adalah dengan memalsukan identitas pengirim pada saat pengiriman barang. Dengan terjadinya kasus pemalsuan identitas atas pengiriman narkotika jenis sabu ini, pelacakan pelaku pengirim narkotika akan sulit untuk dilacak oleh pihak kepolisian. Beredarnya narkotika jenis sabu di masyarakat oleh oknum—oknum tidak bertanggung jawab tentunya akan membuat dampak negatif.

Kasus yang serupa terjadi pada tahun 2019 berupa peredaran paket misterius berupa majalah yang menceritakan salah satu pasangan calon presiden dan wakil

presiden pada pemilihan presiden tahun 2019. Paket yang dikirimkan melalui PT.Pos Indonesia ini tidak memiliki informasi mengenai data pengirim[2)]. Dengan beredarnya paket majalah ini dapat menimbulkan pengkotakan pemikiran di masyarakat mengenai pemilihan presiden tahun 2019.

Terjadinya kasus seperti diatas tidak menutup kemungkinan pengiriman barang ilegal lainnya melalui jalur perusahaan pengiriman kembali terjadi. Pengiriman barang ilegal baik dengan menggunakan identitas asli maupun identitas palsu dapat berakibat buruk di masyarakat, dan mempersulit pihak yang berwenang untuk melakukan penyelidikan terhadap pelaku.

Pada tahun 2019 PT.Pos Indonesia regional Palembang mengembangkan sebuah mesin antrian dengan memanfaatkan teknologi RFID (*Radio-Frequency Identification*) yang telah banyak beredar di masyarakat mulai dari kunci ruangan berbasis kartu hingga uang elektronik berbentuk kartu. Penggunaan teknologi RFID ditujukan untuk modernisasi sistem antrian layanan PT. Pos Indonesia. Dengan menggunakan sistem antrian yang baru, seluruh data pelanggan yang berkaitan dengan pelayanan PT. Pos Indonesia akan disimpan di dalam kartu RFID yang dimiliki oleh pelanggan PT. Pos Indonesia sehingga pelanggan tidak perlu memberikan identitas pribadi kepada petugas PT. Pos Indonesia untuk melakukan transaksi layanan yang disediakan.

---

1) Artikel berita “TribunNews”,15 Mei 2017

2) Artikel berita “IslamPos”,25 Januari 2019

Pada sistem antrian yang baru pada PT. Pos Indonesia, seluruh data pelanggan akan disimpan didalam kartu RFID yang telah didaftarkan oleh pihak PT. Pos Indonesia. Pada sistem yang telah dilakukan modernisasi ini, tidak menutup kemungkinan untuk terjadinya aksi yang sama berupa pemalsuan identitas dengan cara merubah data pelanggan yang ada pada kartu RFID kembali terjadi.

Untuk menanggulangi transaksi layanan dengan data pelanggan palsu, maka dikembangkan suatu prosedur otentikasi yang melibatkan data pelanggan pada kartu RFID dan algoritma MD5 (*Message Diggest 5)* untuk menjamin keaslian data pada kartu RFID. Data hash kartu RFID akan disimpan pada basis data PT. Pos Indonesia pada saat pendaftaran dan prosedur otentikasi akan dilakukan pada saat pelanggan melakukan pendaftaran layanan, jika hasil otentikasi adalah benar, maka pelanggan akan diperkenankan untuk melakukan pendaftaran layanan, dan jika hasil otentikasi adalah salah, maka pelanggan akan diarahkan pada layanan *cutomer service* untuk ditindak lanjuti oleh pihak PT. Pos Indonesia. Dengan menggunakan prosedur ini diharapkan proses pelayanan pada PT. Pos Indonesia lebih terjamin keamanannya tanpa mengganggu waktu pada saat pendaftaran transaksi layanan.

Pada penelititan sebelumnya metode otentikasi menggunakan algoritma *hash* MD5 telah diterapkan pada otentikasi pesan singkat pada ponsel (Pairin, 2018) dan *Web-Based Transaction* untuk mengotentikasi kombinasi PIN (*Personal Indetification Number*) dan *challenge number* (Sari, 2010). Pada penelitian ini akan digunakan algoritma yang sama yaitu algoritma *hash* MD5 (*Message Diggest 5)* dalam menjaga integritas data dan proses otentikasi data pelanggan PT.POS Indonesia. Penggunaan algoritma ini dianggap tepat dikarenakan tingkat kecepatan

dan akurasi dalam melakukan *hash* data yang tinggi. Algoritma ini juga dianggap lebih ramah dalam penyimpanan data *hash*, karena menghasilkan sidik digital data pelanggan yang berukuran 128 bit(Cao & Yang, 2010) yang jika dibandingkan dengan algoritma *hash* sha-1 yang dapat membuat sidik data sebesar 160bit (Kurniawan, Kusyanti, & Nurwarsito, 2017).

1.3 Rumusan Masalah

Berdasarkan latar belakang diatas, permasalahan yang timbul adalah bagaimana penerapan algoritma MD5 dalam mengamankan integritas data, dan otentikasi pada keaslian data pelanggan.

1.4 Tujuan Penelitian

Adapun tujuan penelitian ini adalah sebagai berikut:

1. Mengembangkan skema pengamanan intergritas dan otentikasi data pelanggan yang berada pada basis data PT.POS Indonesia.
2. Mengembangkan aplikasi yang dapat melakukan otentikasi terhadap keaslian data pelanggan PT.POS Indonesia dengan menggunakan algoritma MD5.
3. Menguji skema yang telah dibuat dengan aplikasi yang telah dibangun.

1.5 Manfaat Penelitian

Penelitian ini bermanfaat untuk menjaga dan menjamin keaslian data pelanggan PT.POS Indonesia ,sehingga dapat mendeteksi penggunaan data palsu dalam transaksi pelayanan PT.POS Indonesia .

1.6 Batasan Masalah

Batasan masalah yang didefiniskan untuk melaksanakan tugas akhir ini adalah sebagai berikut:

1. Aplikasi hanya melakukan *hash* terhadap kombinasi data—data pelanggan yang sensitif tanpa mengikutsertakan UID (*Unique Identifier*) kartu RFID.
2. Aplikasi tidak menanggulangi kartu pelanggan duplikat.
3. Aplikasi tidak menanggulangi pengembalian data yang telah diubah.

1.7 Sistematika Penulisan

Sistematika Penulisan penelitian ini akan disusun dengan rangkaian sebagai berikut:

1. BAB I Pendahuluan

   Pada bab ini akan dijelaskan mengenai latar belakang, rumusan masalah, tujuan, manfaat , Batasan penelitian dan sistematika penelitian.
2. BAB II Tinjauan Pustaka

   Pada bab ini berisikan penjelasan mengenai landasan teori yang berkaitan dengan penelitian.
3. BAB III Analisis dan Perancangan

   Pada bab ini akan dibahas mengenai tahapan yang akan dilaksanakan pada penelitian. Setiap perencanaan tahapan penelitian akan dideskripsikan dengan acuan kerangka kerja, dan pada akhir bab berisikan manajemen proyek penelitian.

1.8 Kesimpulan

Pada bab ini telah dijelaskan mengenai latar belakang permasalahan yang akan diselesaikan yaitu mengenai pemananan integritas dan otentikasi data pelanggan PT.Pos Indonesia sehingga dapat mendeteksi pelanggaran pemalsuan data pelanggan dengan menggunakan algoritma MD5 (Message digest 5).

DAFTAR PUSTAKA

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

Cao, D., & Yang, B. (2010). Design and implementation for MD5-based data integrity checking system. *ICIME 2010 - 2010 2nd IEEE International Conference on Information Management and Engineering*, *2*, 608–611. https://doi.org/10.1109/ICIME.2010.5477912

Imam Santoso, K., Sediyono, E., & Suhartono, S. (2013). Studi Pengamanan Login Pada Sistem Informasi Akademik Menggunakan Otentifikasi One Time Password Berbasisis SMS dengan Hash MD5. *Jurnal Sistem Informasi Bisnis*, *3*(1), 7–12. https://doi.org/10.21456/vol3iss1pp07-12

Kurniawan, F., Kusyanti, A., & Nurwarsito, H. (2017). Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *1*(9), 803–812.

Laxman Karandikar, R. (2018). Introduction to cryptography. *Selected Readings on Information Technology Management: Contemporary Issues*, 178–191. https://doi.org/10.4018/978-1-60566-092-9.ch011

Mishra, S., Mishra, S., & Kumar, N. (2013). Hashing Algorithm : MD5, *1*(9), 931–933.

Pairin, Y. Bin. (2018). Kode Autentikasi Hash pada Pesan Teks Berbasis Android.

Eksplora Informatika, *8*(1), 6. https://doi.org/10.30864/eksplora.v8i1.129

PUTRA, R. H. P. (2017). IMPLEMENTASI ALGORITMA KRIPTOGRAFI ELGAMAL UNTUK ENKRIPSI DATA TEKS.

Rivest, R. (1992). The MD5 Message-Digest Algorithm This. *RFC 1321 :The MD5 Message-Digest Algorithm*.

Sari, Y. S. D. (2010). Autentikasi Dengan Metode MD5 One Way Hash Function Challenge Response Pada Web-Based Transaction.

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

Yong-Xia, Z., & Ge, Z. (2010). MD5 research. *2010 International Conference on MultiMedia and Information Technology*, *MMIT 2010*, *2*, 271–273. https://doi.org/10.1109/MMIT.2010.186