PENERAPAN ALGORITMA PGP UNTUK ENKRIPSI CSV FILE DI PT. X

Tugas Akhir

Diajukan untuk Memenuhi Salah Satu Persyaratan Mencapai Derajat Sarjana Informatika

Dibuat Oleh:

RIANDY RAFAEL

16 07 08828

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ATMA JAYA YOGYAKARTA

2020

LEMBAR PENGESAHAN

Penerapan Algoritma PGP untuk Enkripsi CSV *File* di PT. X

Yogyakarta, 07 Juli 2020

Riandy Rafael
16 07 08828

Menyetujui,

Pembimbing I	Pembimbing II
Eddy Julianto, S.T., M.T.	**Paulus Mudjihartono, S.T., M.T., PhD**
Penguji I	**Penguji II**
Dr. Andi Wahju Rahardjo, BSEE., MSSE	**Joseph Eric Samodra, S.Kom, MIT.**

Mengetahui,
Dekan Fakultas Teknologi Industri

Dr. A. Teguh Siswantoro, M.Sc.

PERNYATAAN ORISINALITAS & PUBLIKASI ILMIAH

Saya yang bertanda tangan di bawah ini:

Nama Lengkap	: Riandy Rafael
NPM	: 16 07 08828
Program Studi	: Teknik Informatika
Fakultas	: Teknologi Industri
Judul Penelitian	: Penerapan Algoritma PGP untuk Enkripsi CSV *File* di PT. X

Menyatakan dengan ini:

1. Tugas Akhir ini adalah benar tidak merupakan salinan sebagian atau keseluruhan dari karya penelitian lain.
2. Memberikan kepada Universitas Atma Jaya Yogyakarta atas penelitian ini, berupa Hak untuk menyimpan, mengelola, mendistribusikan, dan menampilkan hasil penelitian selama tetap mencantumkan nama penulis.
3. Bersedia menanggung secara pribadi segala bentuk tuntutan hukum atas pelanggaran Hak Cipta dalam pembuatan Tugas Akhir ini.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 18 Juni 2020

Yang menyatakan,

Riandy Rafael

16 07 08828

PERNYATAAN PERSETUJUAN DARI INSTANSI ASAL PENELITIAN

Saya yang bertanda tangan di bawah ini:

Nama Lengkap Pembimbing : Djoa Danny

Jabatan : HRD Jr. Manager

Departemen : HRD

Menyatakan dengan ini:

Nama Lengkap : Riandy Rafael

NPM : 16 07 08828

Program Studi : Teknik Informatika

Fakultas : Teknologi Industri

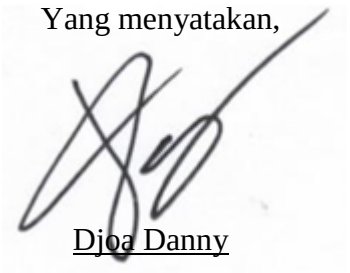
Judul Penelitian : Penerapan Algoritma PGP untuk Enkripsi CSV *File* di PT. X.

1. Penelitian telah selesai dilaksanakan pada perusahaan.
2. Perusahaan telah melakukan sidang internal berupa kelayakan penelitian ini dan akan mencantumkan lembar penilaian secara tertutup kepada pihak universitas sebagai bagian dari nilai akhir mahasiswa.
3. Memberikan kepada Instansi Penelitian dan Universitas Atma Jaya Yogyakarta atas penelitian ini, berupa hak untuk menyimpan, mengelola, mendistribusikan, dan menampilkan hasil penelitian selama tetap mencantumkan nama penulis.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Jakarta, 6 Juli 2020

Yang menyatakan,



Djoa Danny

-

HALAMAN PERSEMBAHAN

Penelitian ini tidak akan selesai tanpa berkat dari Tuhan Yang Maha Esa dan dukungan dari orang-orang terdekat yang mendukung saya dalam menyelesaikan tugas akhir ini. Sebagai bentuk rasa syukur saya ingin berterimakasih kepada:

1. Papa, mama, adik, kakak, dan seluruh anggota keluarga besar yang selalu mendoakan yang terbaik dan selalu memberi dukungan hingga diselesaikanya tugas ini.
2. Yuri Amelia yang selalu menjadi motivasi saya untuk terus maju dan tidak pernah lelah untuk memberi koreksi dan dukungan bagi saya baik secara fisik dan mental.
3. Teman-teman saya di kampus, teman-teman saya di SMA, dan teman-teman saya yang lain dimanapun kalian berada yang selalu saling mendukung serta menghibur satu sama lain.
4. Dosen-dosen pada Universitas Atma Jaya Yogyakarta yang selalu memberi pengajaran yang terbaik bagi kami, dan juga dukungan secara teknis sehingga kami dapat ilmu yang sangat berharga.
5. Bapak Ir. A. Djoko Budiyanto SHR, M.Eng., Ph.D. selaku dosen pembimbing akademik, bapak Eddy Julianto, S.T., M.T. selaku dosen pembimbing satu, dan bapak Paulus Mudjihartono, S.T., M.T. selaku dosen pembimbing dua.
6. HIMAFORKA yang menjadi tempat saya dalam membangun kepercayaan diri, serta anggota-anggota yang saling membangun satu sama lain.

KATA PENGANTAR

Puji dan syukur penulis haturkan kepada Tuhan Yang Maha Esa karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan pembuatan tugas akhir "Penerapan Algoritma PGP untuk Enkripsi CSV *File* di PT. X" ini dengan baik.

Penulisan tugas akhir ini bertujuan untuk memenuhi salah satu syarat untuk mencapai derajat sarjana Teknik Informatika dari Program Studi Teknik Informatika, Fakultas Teknologi Industri di Universitas Atma Jaya Yogyakarta.

Penulis menyadari bahwa dalam pembuatan tugas akhir ini penulis telah mendapatkan bantuan, bimbingan, dan dorongan dari banyak pihak. Untuk itu, pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Tuhan Yesus Kristus yang selalu membimbing dalam iman-Nya, memberikan berkat-Nya, dan menyertai penulis selalu.
2. Bapak Dr. A. Teguh Siswantoro, M.Sc., selaku Dekan Fakultas Teknologi Industri, Universitas Atma Jaya Yogyakarta.
3. Bapak Eddy Julianto, S.T., M.T., selaku dosen pembimbing I yang telah membimbing dan memberikan masukan serta motivasi kepada penulis untuk menyelesaikan tugas akhir ini.
4. Bapak Paulus Mudjihartono, S.T., M.T., selaku dosen pembimbing II yang telah membimbing dan memberikan masukan serta motivasi kepada penulis untuk menyelesaikan tugas akhir ini.

Demikian laporan tugas akhir ini dibuat, dan penulis mengucapkan terima kasih kepada semua pihak. Semoga laporan ini dapat bermanfaat bagi pembaca.

Yogyakarta, 15 Maret 2018

Riandy Rafael

16 07 08828

DAFTAR ISI

LEMBAR PENGESAHAN ii
PERNYATAAN ORISINALITAS & PUBLIKASI ILMIAH..... iii
PERNYATAAN PERSETUJUAN DARI INSTANSI ASAL PENELITIAN iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI..... vii
DAFTAR GAMBAR x
DAFTAR TABEL..... xii
INTISARI..... xiii
BAB I. PENDAHULUAN.....1
1.1. Latar Belakang 1
1.2. Rumusan Masalah 2
1.3. Batasan Masalah.....2
1.4. Tujuan Penelitian 2
1.5. Metode Penelitian.....2
BAB II. TINJAUAN PUSTAKA.....4
BAB III. LANDASAN TEORI.....9
3.1. Pretty Good Privacy 9
3.2. Web Service.....10
3.3. Representational State Transfer.....11
3.4. ASP.NET 11
3.5. VB.NET 12
3.6. Comma Separated Values File 12
BAB IV. ANALISIS DAN PERANCANGAN SISTEM.....14
4.1. Analisis Sistem.....14
4.2. Lingkup Masalah.....15

4.3. Perspektif Produk 15
4.4. Fungsi Produk 16
4.4.1. *Use Case Generate Key File* 17
4.4.2. *Use Case Encrypt File* 17
4.4.3. *Use Case Decrypt File* 19
4.4.4. *Use Case Encrypt and Sign File* 21
4.4.5. *Use Case Decrypt and Verify File* 22
4.4.6. *Use Case Generate Key* 25
4.4.7. *Use Case Encrypt* 25
4.4.8. *Use Case Decrypt* 26
4.4.9. *Use Case Encrypt and Sign* 27
4.4.10. *Use Case Decrypt and Verify* 28
4.5. Kebutuhan Antarmuka 29
4.5.1. Antarmuka Pengguna 29
4.5.2. Antarmuka Perangkat Keras 30
4.5.3. Antarmuka Perangkat Lunak 31
4.5.4. Antarmuka Komunikasi 32
4.6. Perancangan 32
4.6.1. Perancangan Arsitektur 32
4.6.2. Perancangan Antarmuka 35
4.6.2.1. Antarmuka *Home Page* 36
4.6.2.2. Antarmuka Generate Key 36
4.6.2.3. Antarmuka Encrypt File 38
4.6.2.4. Antarmuka Decrypt File 39
4.6.2.5. Antarmuka Encrypt and Sign File 41

4.6.2.6. Antarmuka Decrypt and Verify File 42
BAB V. IMPLEMENTASI DAN PENGUJIAN SISTEM 44
5.1. Implementasi Sistem Implementasi Antarmuka 44
5.2. Pengujian Fungsionalitas Perangkat Lunak 65
5.3. Hasil Pengujian Terhadap Pengguna 103
BAB VI. PENUTUP 106
6.1. Kesimpulan 106
6.2. Saran.....106
DAFTAR PUSTAKA 107

DAFTAR GAMBAR

Gambar 4.1 Diagram Use Case Sistem Penerapan Algoritma PGP untuk enrkripsi CSV File di PT. X 16
Gambar 4.2. Arsitektur Sistem 33
Gambar 4.3. Arsitektur Perangkat Lunak 34
Gambar 4.4. *Deployment* diagram 35
Gambar 4.5. Antarmuka *Home Page* 36
Gambar 4.6. Antarmuka *Generate Key* 37
Gambar 4.7. Pseudocode Generate Key 37
Gambar 4.8. Antarmuka *Encrypt File* 38
Gambar 4.9. *Pseudocode Encrypt File* 39
Gambar 4.10. Antarmuka *Decrypt File* 40
Gambar 4.11. *Pseudocode Decrypt File* 40
Gambar 4.12. Antarmuka *Encrypt and Sign File* 41
Gambar 4.13. *Pseudocode Encrypt and Sign File* 42
Gambar 4.14. Antarmuka *Decrypt and Verify File* 43
Gambar 4.15. *Pseudocode Decrypt and Verify File* 43
Gambar 5.1. Tampilan antarmuka *Form Home* 44
Gambar 5.2. Tampilan Antarmuka *Form Generate Key* 45
Gambar 5.3. Tampilan Antarmuka *Form Encrypt and Sign* 46
Gambar 5.4. Tampilan Antarmuka *form Decrypt and Verify* 47
Gambar 5.5. Tampilan Antarmuka *Form Encrypt File* 48
Gambar 5.6. Tampilan Antarmuka *Form Decrypt* 49
Gambar 5.7. Contoh Tampilan CSV *File* 50
Gambar 5.8. Contoh *File Public Key* 51
Gambar 5.9. Contoh *File Private Key* 51
Gambar 5.10. Contoh *Header File* PGP 52
Gambar 5.11. Contoh *Footer File* PGP 53
Gambar 5.12. *Code* pada *Encrypt Controller* 55

Gambar 5.13. *Code* pada *Decrypt Controller* 55
Gambar 5.14. *Code* pada *Key Controller*.....55
Gambar 5.15. *Code* pada kelas *Key* 56
Gambar 5.16. *Code* prosedur *encrypt* pada kelas *Encrypt* bagian pertama 57
Gambar 5.17. *Code* prosedur *encrypt* pada kelas *Encrypt* bagian kedua.....57
Gambar 5.18. *Code* fungsi membaca *public key* pada kelas *Encrypt* 58
Gambar 5.19. *Code* prosedur *Decrypt* pada kelas *Decrypt* bagian pertama 59
Gambar 5.20 *Code* prosedur *Decrypt* pada kelas *Decrypt* bagian kedua.....59
Gambar 5.21 *Code* fungsi mencari *secret key* pada kelas *Decrypt*.....59
Gambar 5.22 *Code* prosedur *EncryptandSign* pada kelas *Encrypt and Sign*. 60
Gambar 5.23 *Code* prosedur *OutputEncrypted* pada kelas *Encrypt and Sign*. 60
Gambar 5.24 *Code* fungsi untuk membuat *Symmetric Key* dan menambah *Public Key* pada kelas *Encrypt and Sign*. 61
Gambar 5.25 *Code* fungsi menambah identitas pada pesan dalam kelas *Encrypt and Sign*.....61
Gambar 5.26 *Code* prosedur *untuk menulis* pesan terenkripsi pada kelas *Encrypt and Sign*.....61
Gambar 5.27 *Code* prosedur DecryptAndVerify pada kelas *Decrypt and Verify*..62
Gambar 5.28 *Code* fungsi untuk mencocokan *public key*.....62
Gambar 5.29 *Code* untuk dekripsi dan membersihkan pesan 63

DAFTAR TABEL

Tabel 2.1. Tabel Pembanding Kajian Pustaka 7
Tabel 5.1. Pengujian Integritas *File* dengan *Hash Compare* 63
Tabel 5.2. Pengujian Fungsionalitas Perangkat Lunak Secara Manual 66
Tabel 5.3. Tabel Pengujian terhadap sistem enkripsi CSV *file* mengunakan algoritma PGP terhadap pengguna. 103

INTISARI

PENERAPAN ALGORITMA PGP UNTUK ENKRIPSI CSV FILE DI PT. X

Riandy Rafael

16 07 08828

PT. X adalah perusahaan yang bergerak di bidang retail Indonesia. Perusahaan retail pasti memiliki banyak sekali data yang bersifat sensitif, seperti data penjualan, data pegawai, dan berbagai data lainya. Data yang dimiliki, seringkali dikirimkan melalui internet, untuk berbagai macam kebutuhan. Data yang dikirimkan tersebut selalu memiliki peluang untuk dicuri oleh orang yang tidak bertanggung jawab. Pencurian data ini dapat berdampak pada kerugian dari masyarakat dan perusahaan. Salah satu cara untuk melindungi data dari pencurian adalah dengan melakukan enkripsi, sehingga data menjadi tersamarkan ketika dikirimkan lewat internet, dan hanya pihak tertentu saja yang dapat membaca data tersebut.

Untuk menanggulangi hal keamanan data ini, digunakan metode enkripsi PGP (*Pretty Good Privacy)*. Sistem yang dibentuk adalah berupa aplikasi *desktop* yang terhubung *web server* dimana fungsi enkripsi disimpan. Pemanggilan fungsi enkripsi ini menggunakan *web service*. Aplikasi *desktop* menjadi antarmuka untuk pengguna serta penghubung *web service* dengan pengguna, agar enkripsi dapat dilakukan. Enkripsi dilakukan dengan cara enkripsi dua arah.

Dari hasil pengembangan, enkripsi data yang dimiliki PT. X yang menggunakan sistem enkripsi PGP telah meningkatkan keamanan data yang dikirim melalui internet. Pembuatan enkripsi PGP versi *desktop* ini terbukti mempermudah dan mempercepat proses enkripsi data. Tingkat kepuasan pengguna untuk sistem ini adalah 4.5 dari skala 5.

Kata Kunci: Enkripsi, PGP, VB.NET.

Dosen Pembimbing I : Eddy Julianto, S.T., M.T.

Dosen Pembimbing II : Paulus Mudjihartono, S.T., M.T.

Jadwal Sidang Tugas Akhir : xxx

BAB I. PENDAHULUAN

1.1. Latar Belakang

Pada jaman sekarang ini, kita sangat mengandalkan teknologi untuk membantu kehidupan kita. Tidak jarang juga teknologi yang kita gunakan dapat membawa keuntungan berupa uang ataupun potongan harga. Namun, jika ingin mendapatkan keuntungan tersebut, kita harus memberitahu beberapa informasi yang bersifat pribadi dan sensitif. Salah satu kasus kebocoran data di salah satu media sosial pada April 2018 lalu memakan korban lebih dari 50 juta pengguna. Data yang bocor dapat digunakan secara tidak bijak oleh orang-orang yang tidak bertanggung jawab. Lemahnya pegamanan ini bahkan dapat membuat kerugian yang besar, seperti dalam kasus Coinrail yang merupakan sebuah perusahaan yang bergerak di pertukaran *cryptocurrency*, mengalami kerugian akibat diretas oleh *hacker* sebesar 35 juta *dollar* AS. Salah satu kasus serupa juga terjadi di Jepang dalam perusahaan CoinCheck dimana koin seharga 500 juta *dollar* AS dicuri [1].

Kasus-kasus yang terjadi tidak selalu terjadi dalam perusahaan pertukanaran uang ataupun. Menurut penelitian, kasus yang terjadi bahkan bsia menimpa perusahaan yang bergerak di bidang kesehatan dan asuransi. Peretas berusaha mengambil data dari perusahaan bidang tersebut karena data yang dimiliki oleh perusahaan yang bergerak dibidang tersebut sangat sensitif. Data-data seperti rekaman kesehatan dan nomor keaman sosial dapat menyebabkan pencurian identitas oleh peretas [2].

PT. X adalah sebuah perusahaan yang bergerak di bidang retail di Indonesia. Perusahaan pasti menginginkan keamanan yang maksimal untuk setiap data yang dipercayakan kepada mereka. Dalam mengirimkan data, perusahaan menggunakan *file comma-separated values* atau CSV. Oleh karena itu ada suatu algoritma yang digunakan oleh sistem untuk mengenkripsi data-data pada perusahaan. Fungsi dari enkripsi data adalah untuk menyamarkan tulisan yang hendak dibaca, sehingga memiliki karakter yang acak. Pada penelitian ini, penulis akan menggunakan algoritma PGP untuk menjadi lapisan pertahanan melawan peretasan sistem. PGP

adalah salah satu algoritma enkripsi yang umumnya digunakan untuk enkripsi data berupa *e-mail* atau *file* teks [3].

Algoritma PGP menjadi salah satu pilihan untuk melakukan enkripsi *file* dengan keamanan yang baik, karena penggunaan 2 kunci yaitu *symmetric* dan *asymmetric* untuk enkripsi suatu data. Data akan dienkripsi menggunakan kunci *public* dari *keypair* yang dikirimkan penerima pesan. Setelah berhasil dienkripsi, selanjutnya data yang terenkripsi akan diterima penerima, data yang diterima hanya bisa di dekripsi kembali menggunakan kunci *private* dari pasangan kunci yang terlah dikirimkan.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang sudah dijelaskan maka dapat dibuat suatu rumusan masalah yaitu bagaimana meningkatkan keamanan perpindahan data untuk *file* CSV yang berisi informasi transaksi di PT.X.

1.3. Batasan Masalah

Karena aspek yang sangat banyak dalam penelitian ini maka diperlukan batasan masalah dalam proses pembuatan skripsi ini yaitu:

1. Sistem yang dibuat berupa fungsi dan implementasi dalam *desktop*, fungsi yang dibuat dapat dipanggil menggunakan web API.
2. Data yang di enkripsi berupa *comma-seperated values file*.

1.4. Tujuan Penelitian

Data yang dikirimkan sangat mudah untuk dicuri dan disalahgunakan oleh pihak tidak bertanggung jawab. Oleh karena itu penelitian ini bertujuan untuk menerapkan algoritma PGP untuk enkripsi CSV *file* di PT.X untuk meningkatkan keamanan pengiriman data perusahaan.

1.5. Metode Penelitian

Beberapa metode yang akan digunakan dalam penelitian ini adalah:

1.5.1. Kajian Pustaka

Proses kajian pustaka meliputi proses pembandingan penelitian dalam membuat sistem ini dengan penelitian yang sudah pernah dilakukan sebelumnya oleh penulis lain.

1.5.2. Perancangan

Proses perancangan perangkat lunak untuk membuat sistem semakin efektif dalam menyelesaikan masalah, dan juga membuat sistem yang akan dibuat semakin efektif dan aman.

1.5.3. Pengkodean Sistem

Proses ini meliputi mengaplikasikan perancangan sistem yang telah dibuat sebelumnya. Perancangan diterapkan dalam pengkodean sistem sebagai inti utama pengerjaan penelitian ini.

1.5.4. Pengujian

Proses pengujian adalah proses percobaan enkripsi CSV *file* yang diuji dengan implementasi melalui sistem aplikasi desktop.

1.6. Sistematika Penulisan

Sistematika penulisan laporan ini disusun sebagai berikut :

BAB I : PENDAHULUAN

Bab pertama yang berisi pendahuluan akan mencakup latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan. Pada bab ini akan dijelaskan alasan dari pelaksaan penelitian, permasalahan yang hendak diselesaikan, penjelasan secara singkat metode yang akan dilakukan

BAB II : TINJAUAN PUSTAKA

Bab kedua adalah tinjauan pustaka yang berisi tentang penelitian yang telah dilakukan sebelumyna sebagai referensi untuk membandingkan penelitian ini dengan penelitian terdahulu. Tabel perbandingan juga disertakan sebagai media

untuk memperjelas perbandingan antara penelitian terdahulu, dengan penelitian ini.

BAB III : LANDASAN TEORI

Bab ketiga yang berisi landasan teori akan menjelaskan pengertian mengenai algoritma, ataupun arsitektur perangkat lunak yang digunakan. Segala sesuatu yang bersifat teknis yang digunakan di dalam penelitian ini akan dijelaskan secara lebih mendetil untuk mengetahui makna dan kegunaanya di dalam penelitian ini.

BAB IV : ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini akan dijelaskan tentang rancangan sistem oleh penulis. Perihal yang dibahas adalah analisis sistem, lingkup masalah, perspektif produk, fungsi produk, pernacangan arsitektur serta perancangan antarmuka. Terdapat tabel yang akan menjelaskan mengenai fungsi yang akan dibuat, esrta diagram untuk memperjelas alur sistem.

BAB V : IMPLEMENTASI MODEL DAN PENGUJIAN SISTEM

Untuk bab kelima akan dijelaskan mengenai implementasi sistem serta pengujianya terhadap pengguna. Pada bab ini akan dijelaskan mengenai implementasi sistem, implementasi antarmuka, pengujian fungsionalitas, dan hasil pengujian terhadap pengguna. Dalam bagian ini terdapat berbagai gambar mengenai antarmuka, serta potongan *code* yang penting, dan juga tabel mengenai hasil pengujian fungsionalitas, maupun tabel hasil pengujian dari pengguna.

BAB VI : KESIMPULAN

Pada bab kesimpulan akan dijalskan temuan yang didapat dari proyek yang telah dibuat. Akan dijelaskan juga mengenai saran-saran yang menurut penulis bisa menjadi pengembangan pada pnelitian yang dilakukan untuk masa mendatang.

BAB II. TINJAUAN PUSTAKA

Penelitian menerapkan algoritma PGP sebelumnya telah dikerjakan oleh beberapa peneliti sebelumnya. Hasil dari penelitian mereka digunakan sebagai referensi untuk penelitian-penelitian serupa di masa mendatang. Ini adalah beberapa penelitian sebelumnya sebagai pembanding dari penelitian ini.

Dandy, dan Ida telah melakukan penelitian dalam melakukan implementasi keamanan *e-mail* menggunakan Zimbra *Mail Server*[4]. Mereka melakukan pengamanan *e-mail* dengan memanfaatkan *private key* dan *public key*. Dalam penelitian yang mereka lakukan, mereka membandingkan hasil perbedaan *file* yang dilampirkan dalam *e-mail* untuk setiap jenis *file* yang berbeda. Perbadingan dilakukan dengan membandingkan ukuran file asli dengan ukuran file setelah dilakukan enkripsi PGP dan ketika file tidak dilakukan enkripsi sama sekali. Kesimpulan yang dapat diambil dari penelitian mereka adalah PGP dapat mengamankan komunikasi secara *e-mail*, pihak yang tidak bertanggung jawab yang mungkin mengetahui *password* ataupun *username* pengguna, tetapi pesan tidak dapat terbaca.

Penelitian dilakukan Setiawan untuk mengimplementasikan teknik pengamanan data PGP unuk Mail Server Zimbra untuk keamanan *e-mail* pada Data Center IAIN kota Cirebon [5]. Pada penelitian tersebut mereka mengamankan data *e-mail*, yang sering kali mendapatkan keluhan seringnya diretas oleh pihak-pihak tidak bertanggung jawab. Setiawan melakukan instalasi DNS Bind9 terlebih dahulu, yang kemudian dilaukan instalasi Zimbra sebagai *server* untuk jalur keluar masuknya *e-mail*. Setelah itu ditambahkan *key* untuk *public* dan *private* sebagai bentuk implementasi teknik PGP agar data tidak dapat diretas dengan mudah. Kesimpulan yang diambil dalam penelitian yang dilakukan diatas adalah enkripsi PGP sudah memenuhi tiga indikator keamanan yaitu kerahasiaan, keutuhan, dan keaslian. Indikator kerahasiaan terpenuhi karena penggunaan *private key* dan *public key*. Semetara indikator keutuhan terpenuhi karena data yang dienkripsi, tidak akan berubah isinya, ketika dikembalikan ke *file* aslinya. Indikator keaslian juga

terpenuhi karena yang hanya bisa mentejemahkan *file* tersebut hanyalah orang yang memiliki *private key* pasangan dari *public key* yang digunakan untuk enkripsi *file* tersebut.

Sudarma juga melakukan salah satu penelitian terkait dengan implementasi PGP berupa implementasi keamanan *e-mail* menggunakan PGP dengan *server* Zimbramail [6]. Aplikasi yang digunakan untuk membuat *key* adalah Cleopatra. Ketika *key* di *generate* penerima *key* harus mengingat kata sandi untuk mengakses *key* tersebut, yang berarti *key* bersifat unik dan perlu kejelasan mengenai identitas dari pengguna yang hendak menggunakan *key* teresbut. Cara kerjanya adalah ketika pengirim e-mail hendak mngirimkan e-mailnya, sistem langsung mengenerate *key* yang akan diterima oleh pengirim dan penerima. Setelah *key* diterima, e-mail dikirim dan dienkripsi dengan *private key*. Setelah terkirim, proses pengkodean dilakukan menggunakan *public key*. Ketika pesan sudah sampai, maka pesan akan di dekripsi lagi menggunakan *private key* yang diterima oleh penerima. Ketidakcocokan *private key* yang diterima dapat menyebabkan pesan tidak dapat terbaca, sehingga kalimat menjadi acak-acakan dan tersamarkan. Kesimpulan yang dapat diambil dari penelitian tersebut adalah teknik PGP dapat digunakan untuk mengamankan e-mail. Akun ataupun *password e-mail* mungkin saja bisa dicuri oleh orang tidak bertanggung jawab, tetapi pesan yang terkirimkan tidak bisa dibaca karena sudah di enkripsi. Penggunaan PGP untuk enkripsi pesan, juga memperbesar ukuran pesan, karena penggunaan *key* sebagai pelapis untuk enkripsi data.

Penelitian tentang PGP juga dilakukan oleh Amrul, dkk untuk enkripsi data dalam e-mail situs jurusan teknik elektro *Universitas Muhammadiyah Malang*. Dalam penelitian ini dilakukan pengamanan *multi mail server* menggunakan OpenPGP [7]. Perangkat lunak *multi mail server* yang digunakan disini adalah *Zimbra Collaboration Suite* (ZCS). *Key* yang digunakan untuk enkripsi *e-mail* terdapat dalam masing-masing *server*, sehingga setiap *server* dalam *multi mail server* memiliki *key* yang berbeda-beda. Kesimpulan yang dapat diambil dalam penelitian tersebut adalah adanya perbedaan dalam *header* pesan, *header* yang berbeda memberikan identitas enkripsi. Pesan dengan identitas tersebut dapat dikenali OpenPGP sebagai pesan yang terenkripsi dengan PGP.

Suatu penelitian tentang PGP juga dilakukan oleh Ewi [8]. Dalam penelitian ini dilakukan pengamanan *e-mail* menggunakan enkripsi PGP, untuk melakukan enkripsi PGP Ewi menggunakan perangkat lunak terbuka yang bernama *Gnu Privacy Guard* (GnuPG). Perangkat lunak tersebut mengimplementasikan standar OpenPGP, Perangkat lunak tersebut melakukan pembuatan *key pair*, yang nantinya *public key* akan diberikan kepada pihak yang hendak mengirimkan pesanya. *Key pair* yang dibuat juga meliputi *private key* yang dilindungi dengan *password* untuk menggunakan *private key* tersebut. Kesimpulan yang diambil dalam penelitian tersebut adalah penggunaan enkripsi PGP dapat membuat pengiriman e-mail menjadi lebih aman. Penelitian ini juga menggunakan *Thunderbird* sebagai *mail client*, alasan penggunaan *Thunderbird* adalah berbagai macam *Operation System* menyediakan perangkat lunak ini. Dalam penelitian ini juga digunakan *Squirrelmail* yang berfungsi sebagai *webmail* untuk mendukung pengiriman *e-mail*. Kesimpulan yang didapat yaitu pengirim dapat menandai pesan yang dienkripsi, sehingga penerima bisa dengan yakin bahwa pesan yang diterimanya adalah pesan yang dikirimkan pengirim, pesan yang dikirimkan juga hanya dapat dibaca oleh pemilik *private key*, yang berarti penerima yang sah.

Berdasarkan tinjauan pustaka yang telah dibahas diatas, penulis membuat suatu tabel perbandingan yang berfungsi untuk membandingkan sistem yang dibentuk dari penelitian terdahulu. Berbagai faktor yang dibandingkan adalah jenis penelitian, adanya pemanfaatan API, bahasa pemograman atau *tools* yang digunakan, data yang dienkripsi, dan perusahaan atau sasaran pengguna. Berbagai aspek tersebut akan dimuat dalam tabel dibawah ini.

Tabel 2.1. Tabel Pembanding Kajian Pustaka

Peneliti	Judul Penelitian	Jenis Penelitian	Penggunaan *Web Service*	Bahasa Pemograman /*Tools*	Data yang di enkripsi	Perusahaan / Sasaran pengguna
Dandy, Ida	Implementasi Pengamanan PGP pada Platform Zimbra Mail Server	Implementasi	Tidak ada	Zimbra	*e-mail*	Pribadi
Setiawan	Implementasi Teknik *Pretty Good Privacy* (PGP) pada *Mail Server* Zimbra dengan Metode Enkripsi untuk Keamanan Data E-mail pada Data Center IAIN Syekh Nurjati Kota Cirebon	Implementasi	Tidak ada	Zimbra, DNS Bind9	*e-mail*	Data Center IAIN Syekh Nurjati kota Cirebon
Sudarma	*Implementation of E-mail Security using* PGP *at* Zimbramail Server	Implementasi	Tidak ada	Cleopatra, Zimbra	*e-mail*	Pribadi

Amrul, dkk	Sistem Keamanan *Multi Mail Server* dengan Teknik Enkripsi OpenPGP pada Zimbra *Exchange Open Source Software*	Implementasi	Tidak ada	ZCS	*e-mail*	Universitas Muhammadiyah Malang
Ewi	Kemanan *E-Mail* Menggunakan Metode Enkripsi GnuPG dengan Squirrelmail dan Thunderbird	Implementasi	Web Server Apache	GnuPG, Thunderbird, Squirellmail	*e-mail*	Pribadi
Riandy	Penerapan Algoritma PGP untuk Enkripsi CSV *File* di PT. X.	Implementasi	Web API	Visual Studio, ASP.NET, VB.NET	CSV *Transaction File*	PT. X

BAB III. LANDASAN TEORI

3.1. Pretty Good Privacy

Pretty Good Privacy adalah program komputer yang dikembangkan Phil Zimmermann pada tahun 1980, program ini membuat orang mampu untuk mengirimkan pesan, *e-mail*, ataupun *file* dengan menambahkan fitur kerahasiaan, dan suatu tambahan authentifikasi pengguna yaitu tanda tangan digital. PGP memiliki *session key* yang berfungsi untuk enkripsi data dan pasangan kunci yang dimiliki oleh pengirim dan penerima *file*. PGP memiliki 2 tingkatan kunci, prinsip inilah yang membuat PGP menjadi lebih aman untuk digunakan. Penggunaan PGP berfungsi untuk melindungi kita dari 3 hal, yang pertama adalah privasi, kerahasiaan pada saat perpindahan data pun terjamin sehingga hanya orang yang memiliki kunci yang dapat melihat pesan yang dikirimkan. Kedua adalah integritas yang mampu menjamin data yang dikirimkan dengan data yang diterima tidak memiliki perbedaan, tentu saja tetap bisa dimodifikasi sesuai kehendak pemilik data tersebut. Ketiga adalah otentikasi yang menjamin kepemilikan data yang terkirim. PGP merupakan sistem kriptografi *hybrid*, yang mengkombinasikan fitur-fitur terbaik yang terdapat dalam kriptografi konvensional dan kriptografi kunci publik [9][10].

Hal yang membuat PGP dipertimbangkan sebagai salah satu alternatif untuk keamanan adalah data yang diamankan memiliki jaminan identitas. Sebagai contoh ketika kita hendak mengirimkan data yang dienkripsi, namun data tersebut diambil peretas, dan akhirnya dimodifikasi, penerima pesan dapat memastikan pesan tersebut tidak berasal dari pengirim yang sesungguhnya, karena modifikasi yang dilakukan dapat terlihat dalam struktur *file* [11].

Keunikan PGP dibanding enkripsi lainya adalah penggunaan *Symmetric Key* dan *Asymmetric Key* dalam melakukan enkripsi dan dekripsi suatu pesan. Banyak cara untuk membuat *Asymmetric Key* yang dapat digunakan dalam PGP, seperti RSA, Elgamal, DSA (*Digital Signature Algorithm*), ECDH (Elliptic-curve Diffie-

Hellman). Dalam membuat *Asymmetric Key*, algoritma yang digunakan untuk penelitian ini adalah algoritma RSA, RSA merupakan singkatatan dari Rivest Shamir Adleman yang merupakan penemu algoritma tersebut. Sampai sekarang algoritma RSA dipercaya sebagai algoritma yang sangat baik dalam membuat *Key*, alasanya adalah kunci yang dibuat memuat kunci yang cukup panjang. Dalam melakukan enkripsi, sebelum data dienkripsi dengan *Asymmetric key*, awalnya data akan di enkripsi dengan *Symmetric Key* sekali pakai atau biasa disebut dengan *Session Key*. *Session key* adalah kunci sekali pakai yang dibuat berdasarkan angka secara acak, gerakan *mouse* secara acak, dan sentuhan pada *keyboard* secara acak. Dalam membuat *Symmetric Key* terdapat banyak pilihan algoritma seperti AES (*Advanced Encryption Standard*), DES (*Data Encryption Standard*), *Triple* DES, Cast5, *Blowfish*, SAFER. Dalam penelitian ini kita membuat *Symmetric Key* dengan algoritma AES. Agar data dapat didekripsi kembali, *session key* dimasukan ke dalam pesan yang dienkripsi. Ketika pesan ingin dibaca kembali, maka pesan harus di dekripsi penerima pesan terlebih dahulu, penerima pesan melakukan dekripsi menggunakan *Private Key* dari *Asymmetric Key*, yang kemudian akan mengembalikan *session key*, sehingga pesan bisa di dekripsi kembali. [12].

3.2. Web Service

Web Service adalah sistem perangkat lunak yang dibentuk untuk menjalankan operasi dari mesin ke mesin melalui jaringan. Kegunaan dari *Web Service* adalah untuk mengkoneksikan secara dinamis dari perangkat-perangkat yang sudah diketahui maupun tidak diketahui di dalam satu jaringan komputer. Untuk arsitekturnya, *web service* memodelkan interaksi antara tiga peran yaitu penyedia layanan, konsumen layanan,dan pendagtar layanan [13].

Web service digunakan sebagai fasilitas yang diberikan oleh *web site* yang dapat digunakan dalam sistem yang lain. Sistem yang dapat menggunakan *web service* tidak hanya sebatas sistem yang terikat dalam web, namun seperti sistem dalam perangkat *mobile* ataupun aplikasi *desktop* juga bisa menggunakan layanan tersebut. Untuk dapat menggunakan layanan tersebut dibutuhkan alamat yang speseifik untuk setiap layanan yang disediakan, sehingga pemakaian layanan

disesuaikan untuk kebutuhan sistem [14].

3.3. Representational State Transfer

Representational State Transfer atau disingkat sebagai REST adalah suatu gaya arsitektur dalam mendesain sebuah *web service*, REST memiliki *resource* yang dapat diakses melalui sebuah alamat HTTP URL yang unik. Dengan bantuan REST, klien juga memungkinkan untuk melakukan *request* dari protokol HTTP menggunakan URI. Konsep ini sangat memudahkan pengggunaan fungsi yang sama pada sistem yang berbeda, atau pemanggilan fungsi yang sama pada suatu sistem. Masing-masing alamat URL mengacu kepada program yang akan dieksekusi. REST mengirimkan perintah menuju *web server* menggunakan metode-metode HTTP. Terdapat delapan metode dalam HTTP yang disebut sebagai *request method*, metode itu meliputi GET, POST, PUT, DELETE, OPTIONS, HEAD, TRACE, dan CONNECT. Dalam API REST hanya empat metode yang diambil yaitu GET, POST, PUT, DELETE [15][13].

Konsep yang diterapkan dalam REST adalah perpindahan antar state. Maksud dari perpindahan antar *state* adalah ketika permintaan dikirimkan ke *web server*, *server* akan mengirimkan *state* halaman web yang diminta saat itu menuju *browser* [16].

3.4. ASP.NET

ASP.NET singkatan dari *Active Server Pages* .NET adalah sebuah teknologi layanan web dinamis, aplikasi web, dan XML *web services* yang dikembangkan oleh Microsoft. Aplikasi web yang dibentuk menggunakan ASP.NET dapat membangun suatu sistem yang dinamis, penggunaan ASP.NET juga memungkinkan untuk pembuatan *web service*. ASP.NET pertama kali dirilis pada Januari 2002, sebelumnya belum terdapat *framework* .NET dalam ASP, sehingga hayna disebut sebagai ASP saja [17].

Seperti namanya ASP.NET ini berbasis .NET *framework* dan dibangun diatas *Common Language Runtime* (CLR), sehingga semua bahasa pemrograman .NET

dapat digunakan. Namun bahasa yang paling populer dan paling umum untuk digunakan adalah C# dan Visual Basic.NET. Keunggulan dari penggunaan ASP.NET ini adalah bahasa-bahasa yang kita gunakan didalam proyek kita, seperti VB.NET, C#, C++, bisa kita gunakan tanpa perlu menyesuaikan *syntax* atau tanpa penggantian *syntax*. *Syntax* yang digunakan sama ketika kita membangun *project windows application* [18][19].

3.5. VB.NET

VB.NET merupakan singkatan dari *Visual Basic* .NET. VB.NET adalah sebua bahasa pemrograman *desktop* yang dirilis Microsoft. *Visual Basic* menggunakan *framework* .NET. VB.NET menjadi salah satu bahasa pemrograman yang paling populer untuk digunakan. Visual Basic merupakan salah satu bahasa pemrograman visual seperti Visual C++, Visual Foxpro. Struktur bahasa pemrograman *Visual Basic*, sama dengan struktur bahasa pemrograman *visual* lainya. Versi *Visual Basic* yang sebelum dapat berjalan di .NET *Framework* adalah VB6 yang dijalankan dalam Visual Studio 1998. *Visual Basic* .NET dirilis pada bulan Februari tahun 2002, versi *Visual Basic* tahun 2002 ini dirilis secara bersamaan dengan *framework* .NET 1.0 [20] [21].

Pada tahun 2005 VB.NET menjadi bahasa pemrograman yang paling banyak dipakai *programmer* di seluruh dunia. Keunggulan dari bahasa ini adalah mudah untuk dipahami dan dipelajari, baik untuk awam, maupun untuk yang sudah mahir menggunakan bahasa pemrograman ini. Pengembangan juga masih dilakukan oleh Microsoft untuk memenuhi kebutuhan sesuai perkembangan jaman, seperti salah satu contoh pengembanganya adalah dengan menerapkan model pemrograman berbasis OOP (*Object Oriented Programming*) [22].

3.6. Comma Separated Values File

Comma Separated Values atau biasa disingkat CSV adalah suatu format data, yang setiap data atau *record* di dalamnya dipisahkan dengan koma atau titik koma. Penulisanya yang sederhana, membuat penulisan data mudah dimengerti

ketika dibaca manusia. Selain karena kesederhanaanya, *file* ini juga dapat dibuka menggunakan berbagai macam *text-editor*. Contoh *text-editor* yang biasa digunakan untuk membuka *file* CSV ini adalah Notepad, Word, MS.Excel [23][24].

Karena penulisanya yang sederhana, membuat data yang ditampung dalam file lebih efektif, sehingga tidak menambahkan terlalu banyak ukuran data. File ini memiliki ekstensi file .csv. Data di dalam file .csv juga dapat di import dengan cukup mudah kedalam database, seperti kedalam SQL dan NoSQL [25].

BAB VI. PENUTUP

6.1. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dengan melihat perancangan, implementasi, serta pengujian terhadap pengguna, maka dapat ditarik kesimpulan sebagai berikut:

a. Pembangunan sistem enkripsi di PT. X dengan menggunakan algoritma PGP telah meningkatkan keamanan perpindahan data CSV *file* yang sudah dienkripsi pada media sosial, ataupun media lain.
b. Berdasarkan aspek kecepatan, keamanan, kepraktisan, serta tampilan yang diujikan kepada pengguna, sistem enkripsi CSV *file* dengan algoritma PGP memberikan kepuasan kepada pengguna dengan skor rata-rata 4,5 dari skala satu sampai lima.

6.2. Saran

Setelah membuat sistem enkripsi menggunakan algoritma PGP ini pengguna memberikan timbal balik berupa saran yang dapat dilakukan pada penelitian lanjutan mengenai sistem ini, antara lain:

a. Penggunaan *web service* memiliki resiko untuk gagal dalam proses enkripsi dan dekripsi, dikarenakan koneksi yang harus selalu ada. Untuk penelitian kedepanya disarankan untuk melakukan enkripsi yang mempertimbangkan keterbatasan *bandwidth*.
b. Dalam melakukan enkripsi dan dekripsi perlu dipertimbangkan menerima berbagai pilihan jenis *file*, seperti *file* dokumen *Excel, Word, Power Point,* dan lainya. Pilihan enkripsi juga bisa ditambahkan untuk teks biasa. Dengan demikian, pengguna dapat melakukan enkripsi pada pesan.

DAFTAR PUSTAKA

[1] "Cyber Attack Trends Analysis Volume 01," vol. 01, 2019.

[2] H. Hammouchi, O. Cherqi, G. Mezzour, M. Ghogho, and M. El Koutbi, "Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time," *Procedia Comput. Sci.*, vol. 151, no. 2018, pp. 1004–1009, 2019, doi: 10.1016/j.procs.2019.04.141.

[3] Paryati, "Keamanan Sistem Informasi," *Semin. Nas. Inform. 2008 (semnasIF 2008) UPN "Veteran" Yogyakarta, 24 Mei 2008*, vol. 2008, no. semnasIF, pp. 379–386, 2008, [Online]. Available: http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/743.

[4] D. Pramana Hostiadi and I. B. Suradarma, "Implementasi Pengamanan PGP Pada Platform Zimbra Mail Server," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 8, no. 1, p. 41, 2017, doi: 10.24843/lkjiti.2017.v08.i01.p05.

[5] A. Setiawan, "Implementasi Teknik Pretty Good Privacy (PGP) Pada Mail Server Zimbra Dengan Metode Enkripsi Untuk Keamanan Data Email Pada Data Center IAIN Syekh Nurjati Kota Cirebon," vol. 17, no. 2, pp. 60–64, 2018.

[6] M. Sudarma and D. P. Hostiadi, "Implementation of Email Security using PGP at Zimbramail Server," vol. 13, no. 6, pp. 113–119, 2016.

[7] A. Faruq, Khaeruddin, and M. Lestandy, "Sistem Keamanan Multi Mail Server dengan Teknik Enkripsi OpenPGP pada Zimbra Exchange Open Source Software," vol. 7, no. 3, pp. 501–508, 2020, doi: 10.25126/jtiik.202071869.

[8] E. Ismaredah, "Kemanan E-Mail Menggunakan Metode Enkripsi GnuPG dengan Squirrelmail dan Thunderbird," *J. Penelit. Ilmu dan Teknol. Komput.*, pp. 13–22, 2015, [Online]. Available: https://jurnal.polsri.ac.id/index.php/jupiter/article/view/701.

[9] A. Febrianto and J. Apriani, "Perbandingan Sistem Pengamanan Email Menggunakan Teknik Public Key Encryption dan Pretty Good Privacy (PGP)," *Cendikia*, vol. 13, no. 2, pp. 17–25, 2017, [Online]. Available: https://jurnal.dcc.ac.id/index.php/JC/article/view/318/175.

[10] Alamsyah, “Implementasi Keamanan E-Mail dengan Menggunakan PGPtray,” *Maj. Ilm. Memtek*, vol. 13, pp. 1–9, 2011.

[11] K. Khetade, V. Sable, M. Sail, and P. Sandeep, “Extended Pretty Good Privacy,” *Int. J. Sci. Res. Dev.*, vol. 2, no. 12, pp. 435–439, 2015, [Online]. Available: http://www.ijsrd.com/articles/IJSRDV2I12214.pdf.

[12] S. A. Sarab, “Improve PGP Cryptography Protocol Using Genetic NTRU Technique,” *Iraqi J. Sci.*, vol. 56, no. 3, pp. 2682–2693, 2015.

[13] M. I. Perkasa and E. B. Setiawan, “Pembangunan Web Service Data Masyarakat Menggunakan REST API dengan Access Token,” *J. Ultim. Comput.*, vol. 10, no. 1, pp. 19–26, 2018, doi: 10.31937/sk.v10i1.838.

[14] F. N. Rofiq and A. Susanto, “Implementasi RESTful Web Service untuk Sistem Penghitungan Suara Secara Cepat pada Pilkada,” *Eksplora Inform.*, vol. 6, no. 2, pp. 159–168, 2017, [Online]. Available: https://eksplora.stikom-bali.ac.id/index.php/eksplora/article/view/116/97.

[15] Syafrial and I. Teguh, “Penerapan Metode Representational State Transfer (RESTFULL) Web Services pada Pembuatan KTP dan Kartu Keluarga,” *Ilm. Teknol. - Inf. dan Sains*, vol. 7, no. November, pp. 37–46, 2017, [Online]. Available: https://media.neliti.com/media/publications/288962-penerapan-metode-representational-state-5277640f.pdf.

[16] B. Adi Pranata, A. Hijriani, and A. Junaidi, “Perancangan Application Programming Interface (Api) Berbasis Web Menggunakan Gaya Arsitektur Representational State Transfer (Rest) Untuk Pengembangan Sistem Informasi Administrasi Pasien Klinik Perawatan Kulit,” *J. Komputasi*, vol. 6, no. 1, pp. 33–42, 2018, doi: 10.23960/komputasi.v6i1.1554.

[17] M. O. Raditya, D. Sunaryono, and A. Munif, “Rancang Bangun Ulang Aplikasi MonTA Menggunakan Workflow Framework pada ASP.NET,” *J. Tek. POMITS*, vol. 2, no. 2, pp. A428–A431, 2013, doi: 10.12962/j23373539.v2i2.3871.

[18] L. W. (2009) Purnomo, “Pembangunan Sistem Informasi untuk Restoran REMOSYS (Restaurant Mobile System),” *Tek. Inform. Mob. Comput.*, vol. 1, no. 9, pp. 1689–1699, 2015, doi: 10.1017/CBO9781107415324.004.

[19] N. Alam and M. Amin, “Aplikasi Pemilihan Rute Alternatif Akibat Kemacetan Lalu Lintas di Kota Makassar Menggunakan Google API dan ASP.Net,” *Pekommas*, vol. 18, no. 2, pp. 93–104, 2015, doi: 10.30818/jpkm.2015.1180203.

[20] Nurullah, “Perancangan dan Pembuatan Sistem Informasi Akuntansi pada STMIK U’Budiyah Menggunakan VB.NET,” vol. Banda Aceh, p. STMIK U’Budiyah Indonesia, 2012.

[21] D. S. U. Mardianto, A. S. M. Lumenta, A. M. Rumagit, and A. P. R. Wowor, “Rancang Bangun Aplikasi Toko Menggunakan Visual Basic 9.0 ‘Studi Kasus Roberta Superstore,’” *E-Journal Tek. Elektro Dan Komput.*, vol. 1, no. 2, pp. 1–7, 2012, [Online]. Available: https://ejournal.unsrat.ac.id/index.php/elekdankom/article/view/601.

[22] Defta Afriani, “Perancangan Knowledge Management System dengan SECI Model Pada Layanan Perbaikan AC Mobil di Bengkel Agung Motor Cinere Menggunakan VB.NET,” *Inform. SIMANTIK*, vol. 4, no. 1, pp. 29–35, 2019.

[23] A. Junaidi, “Studi Perbandingan Performansi Antara MongoDB dan MySQL Dalam Lingkungan Big Data,” *Semin. Nas. Teknol. Inf. dan Multimed. 2017*, vol. 2, no. 1, pp. 460–465, 2017.

[24] M. Deviana, “Penggunaan Fusion Chart pada Pembuatan Grafik Hasil Unduhan Situs Wordpress,” *Jur. ILMU Komput. Fak. Mat. DAN ILMU Pengetah. ALAM*, vol. 23, no. 3, p. 6, 2019, doi: 10.5281/zenodo.1477753.

[25] A. Solichin, “MySQL Dari Pemula Hingga Mahir,” *Univ. Budi Luhur, Jakarta*, no. November, pp. 1–117, 2010.

[26] A. Tanoto, “Analisis Keamanan pada Pretty Good Privacy (PGP),” *J. Chem. Eng. Japan*, vol. 28, no. 3, pp. 245–249, 2007, doi: 10.1252/jcej.28.245.