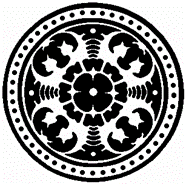
**PROPOSAL TUGAS AKHIR**

**PENERAPAN *NEAR FIELD COMUNICATION* (NFC)**

**SEBAGAI PENGGANTI TIKET KONVENSIONAL**

**PADA BUS TRANS SARBAGITA**



**NYOMAN AGUS WINARTA PALGUNA**

**NIM.1208605087**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**JURUSAN ILMU KOMPUTER**

**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUANALAM**

**UNIVERSITAS UDAYANA**

**BUKIT JIMBARAN**

**2014**

# **DAFTAR ISI**

[DAFTAR ISI ii](#_Toc407169699)

[DAFTAR TABEL ii](#_Toc407169700)

[KATA PENGANTAR iii](#_Toc407169701)

[1. Latar Belakang 1](#_Toc407169702)

[2. Rumusan Masalah 2](#_Toc407169703)

[3. Tujuan Penelitian 2](#_Toc407169704)

[4. Batasan Masalah 2](#_Toc407169705)

[5. Manfaat Penelitian 2](#_Toc407169706)

[6. Tinjauan Pustaka 3](#_Toc407169707)

[6.1 Tinjauan Studi 3](#_Toc407169708)

[6.2. Landasan Teori 5](#_Toc407169709)

[6.2.1.NFC 5](#_Toc407169710)

[6.2.2. Mode Operasi NFC 5](#_Toc407169711)

[6.3. NFC tags 6](#_Toc407169712)

[6.4. Desktop 7](#_Toc407169713)

[6.4. Bus Trans Sarbagita 7](#_Toc407169714)

[6.5. Kriptografi 8](#_Toc407169715)

[6.5.1. Fungsi Hash 8](#_Toc407169716)

[6.5.2 SHA-1 9](#_Toc407169717)

[6.5.3 CARA KERJA SHA - 1 10](#_Toc407169718)

[6.5.4 Kelebihan Algoritma SHAA-1 11](#_Toc407169719)

[7. Metodelogi Penelitian 11](#_Toc407169720)

[7.1. Metode Penelitian 11](#_Toc407169721)

[7.2. Analisis Kebutuhan 12](#_Toc407169722)

[7.3. Perancangan Sistem 12](#_Toc407169723)

[7.4. Pembangunan Sistem 12](#_Toc407169724)

[7.5. Pengujian Sistem 13](#_Toc407169725)

[7.6. Evaluasi dan Analisis Hasil 13](#_Toc407169726)

[DAFTAR PUSTAKA 15](#_Toc407169727)

# **DAFTAR TABEL**

[Table 1 Rincian Komponen sistem 17](#_Toc407169244)

# **KATA PENGANTAR**

Puji syukur peneliti panjatkan kehadirat Tuhan Yang Maha Esa karena atas rahmat-Nya peneliti dapat menyelesaikan proposal Proposal penelitian dengan judul “*Penerapan Near Field Comunication (NFC) Sebagai Pengganti Tiket Konvensional Pada Bus Trans Sarbagita*” inidisusun dalam kegiatan pelaksanaan Tugas Akhir di Jurusan IlmuKomputer FMIPA UNUD. Proposal ini disusun dengan harapan dapat menjadipedoman dan arahan dalam melaksanakan penelitian di atas. Sehubungan dengan telah terselesaikannya proposal ini, maka diucapkan terima kasih dan penghargaan kepada berbagai pihak yang telah membantu penyusunan , antara lain:

1. Bapak Drs. I Wayan Santiyasa, M.Si. selaku Ketua Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Udayana.
2. Komisi Tugas Akhir Jurusan Ilmu Komputer FMIPA UNUD, yang telah memberikan petunjuk dalam penyusunan proposal tugas akhir ini.
3. Rekan-rekan mahasiswa yang telah memberi dukungan, motivasi,semangat dan kerja sama dalam pembuatan proposal tugas akhir ini.
4. Keluarga dan kerabat serta semua pihak yang turut serta memberi dukungan sehingga laporan ini dapat diselesaikan sesuai dengan waktu yang ditentukan.

Penulis menyadari bahwa tugas akhir ini masih belum sempurna, untuk itu kritik dan saran yang bermanfaat demi kesempurnaan tugas akhir ini sangat penulis harapkan.

Denpasar, 19 Desember 2014

Penulis

# **Latar Belakang**

Dewasa ini pertumbuhan mode transportasi sangat pesat, keberadaan transportasi massal yang handal dan memadai sangat dibutuhkan, saat ini transportasi masal masih menggunakan Tiket konvensioanal, Tiket konvensional adalah suatu dokumen perjalanan yang dikeluarkan oleh suatu perusahaan yang berisi rute, tanggal, harga, data penumpang digunakan untuk melakukan suatu perjalanan yang pada awalnya diperuntuk an hanya untuk sekali pakai saja yang dalam penggunaan Tiket ini. masih terdapat banyak kekurangan diantaranya, dalam prakteknya tiket konvensional memerlukan sumberdaya yang kompeten untuk melayani transaksi Tiket dimana dalam transaksi pegawai Bus Trans Sarbagita mengimputkan secara manual total transaksi dan pegawai Bus Trans Sarbagita Harus mengidentifikasi satu per satu kategori penumpang dimana terdapat perbedaan harga Tiket kategori pelajar atau mahasiswa seharga 2500 dan umum 3500 dan masih banyak terjadinya kecurangan pada saat transaksi Tiket konvensional sering kali petugas hanya menerima uang dan tidak memberikan Tiket kepada konsumen. hal tersebut yang mendasari pengembangan teknologi Tiketing ke arah yang lebih baik .

e-Tiket merupakan pegembangan dari Tiket konvensional sebelumnya di dalam e-Ticket tersimpan identitas penumpang, nama penumpang, rute perjalanan kelas tiket, dan harga tiket., pada umummya fungsi e-Tiket sama seperti tiket konvensional perbedaannya terletak pada penambahan fitur keamanan dan flexibelitas . E-tiket dapat digunakan berulang menurut Ardiyanto(2011)

e-Tiket atau electronic ticketing adalah suatu cara untuk mendokumentasikan proses penjualan dari aktifitas perjalanan pelanggan tanpa harus mengeluarkan dokumen berharga secara fisik ataupun paper ticket. Semua informasi mengenai electronic ticketing disimpan secara digital dalam sistem komputer milik perusahaan

Dalam realisasi e-tiket dikembangkanlah suatu teknologi yang disebut Near Field Communication (NFC) . Sistem ini merupakan sistem prabayar dimana uang disimpan di dalam chip yang berbentuk card yang didalamnya dapat menyimpan data seperti ATM, pada kasus BUS Trans Sarbagita *Near Field Communication* (NFC) berperan sebagai pengganti Tiket konvensional dimana dalam transaksi pembayaran natinya dengan menempelkan card Near Field Communication (NFC) pada Reader yang tersedia pada Bus Trans Sarbagita secara otomatis Reader NFC akan membaca sisa dari Tiket. setiap card saat diletakan pada reader jumlah kapasitas Tiket yang ada berkurang satu setiap transaksi disimpan pada desktop dan secara langsung data base akan menyimpan nama pemegang kartu dan kaegori dari penumpang saat e-ticket habis penumpang bisa langsung membeli isi ulang e-Tiket saat berada dalam Bus Trans Sarbagita dengan menghubungi operator yang yang berada di dalam bus trans sarbagita ,Pengembangan teknologi ini mempermudah melakukan transaksi tanpa harus terbatas dengan ruang dan waktu. Metode pembayaran e-Ticket ini merupakan sebuah sistem pembayaran yang memungkinkan kita melakukan transaksi tanpa melibatkan uang secara fisik. Metode ini mulai banyak dikembangkan dengan tujuan mengurangi peredaran uang fisik yang beredar. serta meminimalisir kejahatan yang melibatkan pengguaan uang fisik yang sangat tidak bisa di prediksi.

# **Rumusan Masalah**

Berdasarkan latar belakang yang dijelaskan diatas maka permasalahan yang akan dikaji dalam Tugas Akhir ini adalah bagaimana mengimplementasikan NFC *(Near Field Communication)* sebagai E-Tiketyang akan di terapkan pada Bus Trans Sarbagita sebagai sarana e-Tiket ?

# **Tujuan Penelitian**

Tujuan yang ingin dicapai pada Tugas Akhir ini adalah e-Tiket menggunakan NFC *(Near Field Communication)* pengganti Tiket Konvensional pada Bus Tran Sarbagita.

# **Batasan Masalah**

1. Informasi pengguna tiket yang dienkripsi akan disimpan dalam Tag NFC

aplikasi reader yang terhubung pada komputer.

1. Sistem yang dibuat adalah e-Tiket yang mengutamakan keamanan data
2. Sistem informasi dibuat dengan menggunakan bahasa pemrograman Java.
3. Tag yang digunakan adalah card nfc default
4. Reader yang digunakan ACR-122U.

# **5. Manfaat Penelitian**

1. Mempermudah transaksi pembelian Tiket pada Bus Trans Sarbagita , sehingga mempersingkat waktu untuk melakukan transaksi Pembelian Tiket.
2. Mengurangi resiko kejahatan terhadap penggunaan uang fisik.
3. Mengurangi Peredaran uang kertas
4. Mencegah terjadinya pencurian identitas pengguna yang dapat digunakan

untuk melakukan transaksi digital.

1. Mengimplementasikan teknologi NFC *(Near Field Communication)* Berbasis Desktop dalam Proses Pembayaran Tiket.

# **Tinjauan Pustaka**

## **6.1 Tinjauan Studi**

Pada penelitian ini, penulis menggunakan beberapa jurnal sebagai tinjauan

studi, yaitu sebagai berikut:

Penggunaan Teknologi *Near Field Communication* Pada Telepon Seluler Untuk *Micro Payment* dan *Loyalty Management*

Krisnanda (2013) yang dibahas dalam jurnalnya adalah dalam era kompetisi global yang diperlukan kemampuan untuk mengidentifikasi prioritas dan pilihan pelanggan. Dengan kata lain pengetahuan mengenai pelanggan harus menjadi strategi yang diimplementasikan pada tiap bagian dalam perusahaan, dari tingkat manajemen tertinggi, hingga semua pegawai yang berhubungan langsung dengan pelanggan.*Near Field Communication* adalah teknologi baru yang diperkirakan menjadi tren pada tahun

2011 sampai tahun 2012. Penerapan teknologi ini khususnya padatelepon seluler diharapkan dapat menjawab tantangan globalisasi pasartelekomunikasi dimasa mendatang.

*Implementasi algoritma sistem kriptografi MD5, SHA1, dan RC4 pada aplikasi mobile internet berbasis Java*

Ardyanto(2011) dalam jurnalnya menerangkan bahwa Kebutuhan akan informasi yang mobile menjadi latar belakang bagi perkembangan teknologi proteksi komunikasi data. Ketika membicarakan tentang keamnan data, maka salah satu solusi yang terpikir adalah kriptografi. Kriptografi adalah suatu cabang ilmu matematika yang memanfaatkan proses komputasi untuk mengacak data yang akan dikirimkan. Pada penelitian ini diimplementasikan tiga algoritma yang digunakan dalam kriptografi, antara lain hash function dengan algoritma MD5 dan SHA1, serta algoritma kriptografi simetrik, yaitu RC4. Semua algoritma tersebut diadaptasi ke dalam sistem yang menggunakan platform J2ME. Sistem yang telah diimplementasikan dapat berjalan baik pada emulator J2ME Wireless Toolkit. Analisa terhadap subsistem security dilakukan berdasarkan beberapa parameter, yaitu panjang data aoutput, penggunaan memory, waktu proses, distribusi frekuensi kemunculan karakter, variasi distribusi, avallanche effect untuk algoritma RC4, dan waktu untuk melakukan brute force attack pada algoritma RC4. Dari hasil analisa terhadap parameter- parameter diatas diperoleh bahwa algoritma SHA1 memiliki keunggulan pada parameter panjang data output, waktu proses dengan kombinasi algoritma RC4, distribusi frekuensi, variansi, dan waktu brute force attack. Algoritma MD5 memiliki keunggulan pada parameter penggunaan memory, dan waktu proses tanpa kombinasi algoritma RC4. Maka secara umum algoritma SHA1 memiliki kinerja yang lebih baik daripada MD5.

*Implementasi Teknologi Near Field Communication (NFC) dan Kartu Radio Frequency Identification (RFID) untuk Sistem Resep Dokter berbasis Android*

Putra(2012)menurut yang ditulis pada jurnal ini Resep merupakan media untuk menyimpan informasi obat yang diberikan oleh dokter kepada pasien. Biasanya ditulis menggunakana tulisan tangan pada sebuah media kertas. Near Field Communication (NFC) adalah sebuah hardware yang terdapat di dalam perangkat mobile yang memungkinkan penggunanya membaca dan mengirim data ke dalam tag atau kartu RFID. NFC dan kartu RFID dapat dimanfaatkan untuk membuat sebuah sistem resep dokter berbasis Android. Resep ditulis melalui perangkat Android, kemudian resep ditransfer ke dalam kartu RFID pasien. Selanjutnya pasien memberikan kartu RFID ini kepada petugas apotek. Petugas apotek dengan

menggunakan perangkat Android-nya membaca resep yang terdapat di dalam kartu RFID pasien. Beberapa aplikasi pendukung dibangun untuk mendukung implementasi dari sistem resep dokter ini, seperti aplikasi untuk manajemen daftar obat pada aplikasi dokter dan aplikasi manajemen inventori obat pada apotek. Hasilnya adalah sebuah sistem resep dokter baru dengan menggunakan perangkat Andorid, teknologi NFC dan RFID. Hasil yang didapatkan adalah 96% dokter menyatakatakan bahwa sistem ini dapat mengurangi kesalahan dalam penulisan resep. Persentase apotekerpetugas apotek menyatakan bahwa sistem ini memudahkan mereka dalam bertransaksi dan mencegah terjadinya kesalahan pada data inventori obat apotek adalah sebanyak 76%. Persentase pasien menyatakan bahwa sistem ini memudahkan mereka ketika berobat adalah sebanyak 90%.

## **6.2. Landasan Teori**

### **6.2.1.NFC**

Teknologi *Near Field Communication* (NFC) adalah teknologi nirkabel jarak pendek yang dirancang untuk bertukar dengan cepat, bertukar informasi dikembangkan membuat hidup lebih mudah dan nyaman bagi penggunanya di dalam melakukan transaksi, seperti pertukaran konten [digital](http://id.wikipedia.org/wiki/Digital), hanya menghubungkan perangkat elektronik ke perangkat [elektronik](http://id.wikipedia.org/wiki/Elektronik) yang memiliki teknologi NFC dengan sentuhan, pengguna juga bisa membeli tiket apapun hanya dengan mengaktifkan NFC pada ponsel. Sebuah teknologi konektivitas berbasis standar, NFC memungkinkan memberikan solusi saat ini dan masa mendatang di bidang-bidang seperti Akses kontrol [Konsumen](http://id.wikipedia.org/wiki/Konsumen) [elektronik](http://id.wikipedia.org/wiki/Elektronik)[Kesehatan](http://id.wikipedia.org/wiki/Kesehatan) [Informasi](http://id.wikipedia.org/wiki/Informasi) pengumpulan dan pertukaran Loyalitas dan pembelian kupon Pembayaran[Transportas](http://id.wikipedia.org/wiki/Transportasi)i

NFC adalah seperangkat teknologi konektivitas nirkabel berbasis teknologi RFID *(Radio Frecuency Identification)* yang menggunakan induksi medan magnet untuk memungkinkan komunikasi antar perangkat elektronik dalam jarak yang dekat. NFC dirancang untuk dapat dintegrasikan dengan perangkat *mobile*, yang dapat berkomunikasi antara perangkat *mobile* yang memiliki NFC dengan perangkat *mobile* lainnya *(peer-topeer)* atau membaca informasi di tag dan kartu *(*baca*).* Sebuah perangkat NFC juga dapat dimasukkan dalam mode emulasi kartu, menawarkan kompatibilitas dengan standar *contactless smart card* lainnya. Hal ini memungkinkan perangkat NFC untuk menggantikan kartu plastik *contactless* tradisional yang sering digunakan di depan umum pada tiket transportasi, kontrol akses, ATM dan aplikasi sejenis lainnya.

### **6.2.2. Mode Operasi NFC**

Pada NFC, terdapat tiga mode operasi yang dapat dilakukan pada NFC, yaitu mode Baca*/*Tulis Mode, *Peer-To-Peer* Mode dan *Card Emulation* Mode berikut penjelasan dari ketia mode tersebut

1. Mode P2P *(peer-to-peer),* yang memungkinkan perangkat NFC untuk bertukar data antar perangkat , dengan perangkat lain yang mendungkung NFC. Pada mode ini, dimungkinkan dua buah perangkat NFC pada perangkat *mobile* untuk bertukar informasi, seperti kontak, pesan teks, gambar dan berbagai jenis data lainnya. Mode inimemiliki dua buah standar, yaitu NFCIP-1 dan LLCP.
2. Mode emulasi kartu *(card emulation),* yang memungkinkan perangkat NFC sendiri untuk bertindak sebagai kartu NFC. Kartu NFC yang ditiru kemudian dapat diakses oleh pembaca NFC eksternal.NFC diaktifkan berfungsi sebagai smart card contactless. Mode *card emulation* ini memungkinkan perangkat *TAG* yang terintegrasi dengan NFC diaktifkan berfungsi sebagai smart card contactless. Perangkat *mobile* bahkan dapat menyimpan beberapa contactless aplikasi smart car.
3. Mode baca atau tulis*,* memungkinkan perangkat NFC untuk membaca dan atau menulis tag NFC pasif dan stiker. NFC pada mode ini seperti pada *contactless smart card* dan tag RFID. NFC mendeteksi tag didekatnya dengan menggunakan mekanisme penghindaran tabrakan data antara satu tag dengan tag yang lain yang berada berdekatan dengan baca atau tulis.Sebuah aplikasi pada perangkat NFC dapat membaca membaca data dan menulis data ke tag yang terdeteksi dengan menggunakan mode baca atau tulis.

## **6.3. NFC tags**

NFC tags adalah chip tidak menggunakan tenaga listrik dimana di dalam tag tersimpan data , Untuk terkoneksi NFC perlu menyatukan atau menempelkan dua perangkat NFC.Misalkan saja dengan menempelkan dua perangkat yang mempunyai fitur NFC, saat menempelkan secara back to back. Secara langsung kedua device bertukar data jika menggunakan NFC tags dengan card default NFC cukup tempelkan Card pada reader.

## **6.4. Desktop**

Desktop adalah komputer pribadi yang ditujukan untuk penggunaan secara umum di satu lokasi yang berlawanan dengan komputer jinjing atau komputer portabel. Periferal-periferal komputer meja seperti tampilan komputer, CPU, dan papan ketik terpisah satu sama lain dan relatif berukuran besar (juga berlawanan dengan periferal pada komputer jinjing yang terintegrasi dan berukuran kecil). Komputer jenis ini dirancang untuk diletakkan dan digunakan di atas meja di rumah atau kantor. Komputer meja merupakan komputer yang paling terjangkau dan paling umum digunakan. Komputer adalah alat yang dipakai untuk mengolah [data](http://id.wikipedia.org/wiki/Data) menurut [prosedur](http://id.wikipedia.org/wiki/Prosedur) yang telah dirumuskan.

Kata *computer* pada awalnya dipergunakan untuk menggambarkan orang yang perkerjaannya melakukan perhitungan [aritmatika](http://id.wikipedia.org/wiki/Aritmatika), dengan atau tanpa alat bantu, tetapi arti kata ini kemudian dipindahkan kepada mesin itu sendiri. Asal mulanya, pengolahan informasi hampir eksklusif berhubungan dengan masalah aritmatika, tetapi komputer modern dipakai untuk banyak tugas yang tidak berhubungan dengan [matematika](http://id.wikipedia.org/wiki/Matematika).Dalam arti seperti itu terdapat alat seperti *slide rule*, jenis [kalkulator mekanik](http://id.wikipedia.org/w/index.php?title=Kalkulator_mekanik&action=edit&redlink=1) mulai dari [abakus](http://id.wikipedia.org/wiki/Abakus) dan seterusnya, sampai semua komputer [elektronik](http://id.wikipedia.org/wiki/Elektronik) yang kontemporer. Istilah lebih baik yang cocok untuk arti luas seperti "komputer" adalah "yang mengolah [informasi](http://id.wikipedia.org/wiki/Informasi)" atau "[sistem](http://id.wikipedia.org/wiki/Sistem) pengolah [informasi](http://id.wikipedia.org/wiki/Informasi)."

## **6.4. Bus Trans Sarbagita**

Bus Trans Sarbagita baliprov.go.id (2011) adalah bus angkutan umum antarkabupaten dan kota yang menghubungkan sejumlah trayek di empat wilayah Kabupaten/Kota di Bali, yakni wilayah Kota Denpasar, Kabupaten Badung, Gianyar, dan Tabanan. Nama Sarbagita diambil dari akronim Denpasar (Sar), Badung (Ba), Gianyar (Gi) dan Tabanan (Ta). Pengoperasian bus ini di tahun 2012 telah mampu mengurangi operasional kendaraan bermotor jenis sepeda motor dan mobil sebanyak 1.449 unit per hari. Bus Trans Sarbagita merupakan realisasi nyata dari Program unggulan Bali Mandara yakni Program Trans Sarbagita Pemprov Bali.

Program ini ditangani dengan menerapkan tata kelola transportasi modern dengan tujuan menyediakan dan menyelenggarakan sarana transportasi massal menuju masa depan transportasi Bali yang lebih baik, nyaman dan manusiawi. Dirintis oleh Pemerintah Provinsi Bali di bawah kepemimpinan Gubernur Bali Made Mangku Pastika, bus yang diluncurkan pertama kali pada 17 Agustus 2011 itu kini makin diminati masyarakat, khususnya pelajar dan mahasiswa. Tarif yang jelas dan terjangkau, yakni untuk penumpang umum Rp 3.500 dan untuk pelajar dan mahasiswa Rp 2.500 untuk sekali jalan di trayek utama, Rp 3.000 untuk penumpang umum dan Rp 2.000 untuk pelajar dan mahasiswa untuk trayek pengumpan, serta sebagian besar halte berada di dekat tempat keramaian, menambah daya tarik bus ini.

## **6.5. Kriptografi**

Kriptografi adalah suatu ilmu [yang](javascript:void(0);) mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, [dari](javascript:void(0);) pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data yang disebut dengan enkripsi, Enkripsi adalah kode yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau *chiper*. Sebuah system pengkodean menggunakan suatu *table* atau kamus yang telah didefinisikan untuk mengganti kata dariinformasi atau yang merupakan bagian dari informasi yang dikirim. Sebuah chiper mengunakan suatu algoritma yang dapatmengkodekan semua aliran data (stream) bit dari sebuah pesanmenjadi *cryptogram* yang tidak dimengerti (unintelligible). Karenateknik chiper merupakan suatu system yang telah siap untuk diautomasi, maka teknik ini digunakan dalam system keamanancomputer dan jaringan.Enkripsi dimaksudkan untuk melindungi informasi agar tidak terlihat oleh orang atau pihak yang tidak berhak.

### **6.5.1. Fungsi Hash**

Fungsi hash merupakan fungsi yang menerima masukan bermacam-macam dan menghasilkan string keluaran yang panjangnya tetap. Panjang string keluaran biasanya berukuran jauh lebih kecil daripada ukuran masukan. Fungsi hash satu arah merupakan fungsi hash yang bekerja satu arah, sekali pesan diubah menjadi *message digest*, maka tidak dapat lagi dikembalikan menjadi pesan semula atau *irreversible*. Fungsi hash satu arah harus memenuhi sejumlah kriteria berikut

1. *Preimage resistant*, yaitu tidak mungkin menemukan pesan masukan berdasarkan sebuah message digest.
2. *Second preimage resistant*, yaitu tidak mungkin menemukan dua masukan berbeda yang dapat menghasilkan message digest yang sama.
3. *Collision resistant*, yaitu tidak mungkin menemukan dua pesan masukan dengan nilai hash yang sama.
4. Fungsi hash mudah dihitung.
5. Panjang message digest tetap.
6. Fungsi hash dapat diterapkan paada pesan masukan dengan panjang sebarang

Meskipun fungsi hash satu arah harus memenuhi keenam kriteria tersebut, masih dapat ditemukan sejumlah kolisi pada fungsi hash. Tabel berikut menggambarkan kolisi yang mungkin terjadi secara lebih detil.

### **6.5.2 SHA-1**

SHA-1 atau *Secure Hash Algorithm* didesain oleh *National Security Agent* diperkenalkan oleh NIST sebagai U.S. Federal Information Processing Standard. SHA-1 message digest sepanjang 160 bit. Algoritma utama SHA-1 terdiri dari enam proses utama berikut.

1. Inisialisasi variabel kunci
2. Penambahan bit 1
3. Pemecahan pesan ke dalam kelompok berukuran 512-bit
4. Ekstensi pesan
5. Iterasi utama
6. Pembangkitan hash value.

Hash atau kadang disebut dengan digest adalah semacam tanda tangan untuk sebuah teks atau file data. Sebagai contoh SHA-1 menghasilkan 160 bit tanda tangan untuk sebuah teks.

Hash bukanlah enkripsi – tidak dapat didekripsi untuk mendapatkan teks asli (ia merupakan sebuah fungsi kriptografi satu arah yang memiliki ukuran panjang tertentu yang diperoleh dari teks sumber dengan panjang yang beragam)Hash dapat digunakan oleh beberapa aplikasi untuk :

1. *validate a password* (memvalidasi password); nilai hash dari password akan disimpan, kemudian ketika password diotentikasi, maka password yang dimasukkan oleh user akan dihitung hashnya dan jika hashnya sesuai maka password dinyatakan valid. Namun untuk mendapatkan password yang asli tidak dapat diperoleh dari hash yang telah disimpan.
2. *Challenge handshake authentication;* untuk menghindari kesalahan pengiriman password dalam kondisi “clear”, client dapat mengirim nilai hash sebuah password melalui internet untuk divalidasi oleh server tanpa beresiko disadapnya password yang asli.
3. *anti-tamper* ; untuk memastikan data tidak berubah selama ditransmisikan. Penerima akan menghitung nilai hash dan mencocokkan dengan hash yang dikirimkan, apabila nilainya sama berarti data yang dikirimkan tidak berubah.
4. *digital signatures*; dilakukan dengan cara mengenkrip nilai hash sebuah dokumen dengan menggunakan *private key*, sehingga menghasilkan tanda tangan digital untuk dokumen tersebut. Orang lain dapat mengecek otentikasi dokumen tersebut dengan cara mendekrip tanda tangan tersebut menggunakan *public key* untuk mendapatkan nilai hash yang asli dan membandingkannya dengan nilai hash dari teks.

### **6.5.3 CARA KERJA SHA - 1**

Pesan diberi tambahan untuk membuat panjangnya menjadi kelipatan 512 bit

( l x512 ). Jumlah bit asal adalah k bit. Tambahkan bit secukupnya sampai 64 bit kurangnya dari kelipatan 512 ( 512 – 64 = 448 ), yang disebut juga kongruen dengan 448 ( mod 512 ). Kemudian tambahkan 64 bit yang menyatakan panjang pesan. Inisiasi 5 md variabel dengan panjang 32 bit yaitu a,b,c,d,e. Pesan dibagi menjadi blok-blok berukuran 512 bit dan setiap blok diolah. Kemudian keluaran setiap blok digabungkan dengan keluaran blok berikutnya, sehingga diperoleh output ( diggest ). Fungsi kompresi yang digunakan oleh algoritma sha-1 adalah sebagai berikut : A,b,c,d,e ← ( e + f(t,b,c,d) + s5(a) + wt + kt),a,s30(b),c,d.]

### **6.5.4 Kelebihan Algoritma SHAA-1**

Karena SHA-1 dari MD4 maka SHA-1 mempunyai kemiripan satu sama lain dengan Md5, baik kekuatan dan karakteristiknya. Berikut perbedaan kelebihan SHAA- dengan algoritma Lainnya

1. Keamanan terhadap serangan brute-force. Hal yang paling penting adalah bahwa SHA-1 menghasilkan diggest 32-bit lebih panjang dari algoritma lainnya termasuk MD5.
2. Dengan brute-force maka SHA-1 lebih kuat dibanding MD5. 2. Keamanan terhadap kriptanalisis. Kelemahan MD5 ada pada design sehingga lebih mudah dilakukan kriptanalisis dibandingkan SHA-1
3. Kecepatan. Kedua algoritma bekerja pada modulo 232 sehingga keduanya bekerja baik pada arsitektur 32 bit. SHA-1 mempunyai langkah lebih banyakdibandingkan MD5 ( 80 dibanding MD5 64 ) dan harus memproses 160 bit buffer dibanding DM5 128 bit buffer, sehingga SHA-1 bekerja lebih lambat dibanding MD5 pada perangkat keras yang sama.
4. Simplicity. Kedua algoritma simple untuk dijelaskan dan mudah untuk diiemplementasikan karena tidak membutuhkan program yang besar atau tabel subtitusi yang besar pula

# **Metodelogi Penelitian**

## **7.1. Metode Penelitian**

Desain penelitian yang digunakan adalah dengan desain penelitian eksperimen. Metode ini dipilih dikarenakan perlunya evaluasi akan kecepatan,posisi dan kondisi pembacaan perangkat *Tag* ke Reader secara berulang-ulanguntuk memprediksi kondisi yang paling akurat untuk mekanisme pembacaan oleh Reader sehingga didapatkan hasil yang optimal yang akan digunakan sebagai data analisis.

## **7.2. Analisis Kebutuhan**

Pada sistem pembayaran e-ticket ini, diusulkan untuk menggunakan aplikasi berbasis desktop karena sistem operasi ini mendukung implementasi dari teknologi *Near Field Communication*(NFC) dan menggunakan algoritma HESS SHAA-1 untuk enkripsi data yang disimpan pada aplikasi perangkat tag .

## **7.3. Perancangan Sistem**

Pada tahapan ini, perancangan alur kerja sistem akan dibangun menggunakan flowchart dan workflow untuk mempermudah perancangan sistem.Pengguna akan menggunakan perangkat Tag yang didalamnya terdapat data untuk melakukan proses transaksi keuangan dalam pembayaran e-ticket. Pengguna dapat melakukan top up untuk menambah saldo yang ada pada perangkat Tag mereka, sehingga saldo tersebut dapat digunakan sebagai ticket digital ketika menggunakan fasilitas Bus Trans Sarbagita.

## **7.4. Pembangunan Sistem**

Pada tahapan ini dilakukan implementasi hasil dari rancangan sistem ke dalam baris – baris kode program. Adapun komponen – komponen pendukungy ang digunakan dalam tahap implementasi ini yaitu:

1. Menggunakan sistem operasi Microsoft Windows 8
2. Bahasa pemrograman yang digunakan untuk membangun aplikasi adalah

bahasa pemrograman Java

1. Menggunakan aplikasi yang mendukung bahasa pemrograman Java untuk

membuat sistem

1. Mengimplementasikan algoritma kriptografi HESS SHAA-1 kedalam bahasa

pemrograman Java

1. Melakukan testing hasil program pada perangkat *mobile* dan reader NFC
2. Mendokumentasikan setiap hasil eksperimen.Dalam tahap ini juga terdapat tahap dokumentasi. Dokumentasi akan berisi source code dan bagaimana jalan dari program dan penjelasan dari program yangtelah dibangun. Dengan adanya dokumentasi diharapkan akan membantu dalam pengembangan sistem jika seandainya akan dilakukan pengembangan

## **7.5. Pengujian Sistem**

Menurut Pressman (2010) pengujian *black box* berfokus pada persyaratan Fungsional perangkat lunak yang perekayasa perangkat lunak untuk memperoleh set kondisi input yang sepenuhnya akan melaksanakan persyaratan fungsional untuk sebuah program. Pengujian *black box* berusaha untuk menemukankesalahan dalam kategori berikut:

1. Fungsi yang tidak benar atau fungsi yang hilang

2. Kesalahan antarmuka

3. Kesalahan dalam struktur data atau akses database eksternal

4. Kesalahan perilaku (behavior) atau kesalahan kinerja

5. Inisialisasi dan pemutusan kesalahan

Meskipun didesain untuk mengungkapkan kesalahan, pengujian *black box* digunakan untuk mempelihatkan bahwa fungsi-fungsi perangkat lunak adalahoperasional, yaitu input diterima dengan baik dan output dihasilkan dengan tepat, integritas informasi eksternal dipelihara.

**7.6. Uji Coba**

Dalam uji coba sistem menggunakan berbagai parameter untuk mengetahui efektifitas dari sistem

1. Waktu respon Reader terhadap card NFC.
2. Berapa banyak Costumer yang dapat dilayani dalam satu waktu.
3. Berapa Lama waktu yang diperlukan saat top up.

## **7.7. Evaluasi dan Analisis Hasil**

Melakukan pengujian berdasarkan apa yang dilihat, hanya fokus terhadap fungsionalitas dan output. Pengujian lebih ditujukan pada desain software sesuai standar dan reaksi apabila terdapat celah-celah bug/vulnerabilitas pada program aplikasi tersebut setelah dilakukan white box testing. Proses evaluasi menggunakan Pengujian Black Box, Pengujian Black Box (Pressman, 2010) berfokus pada persyaratan fungsional perangkat lunak yang perekayasa perangkat lunak untuk memperoleh set kondisi input yang sepenuhnya akan melaksanakan persyaratan fungsional untuk sebuah program. Berikut rincian komponen sistem yang akan diuji yang disajikan pada

Table 1 Rincian Komponen sistem

|  |  |  |  |
| --- | --- | --- | --- |
| No | Komponen Sistem | Pengujian | Jenis  Pengujian |
| 1 | Login | Verifikasi kategori | Black Box |
| 2 | Top up saldo e-ticket | Input data top up  Verifikasi data tag | Black box |
| 3 | Cek saldo e-ticket | Inpud data user | Black Box |
| 4 | Transaksi | Input pemotongan e-ticket | Black box |

# **DAFTAR PUSTAKA**

Dudwadkar, A., Gore, A., Nachnani, T., Sabhnani, H. (2013). Near Field Communication in *Mobile* Phone. *International Journal of Engineering* *and Advanced Technology*, 3(1), 2249 – 8958

Candra Alim Sutanto (2012)Algoritma Fungsi Hash Baru dengan Menggabungkan MD5, SHA-1 dan Penyertaan Panjang Pesan Asli 13508069

Made Krisnanda(2012) Penggunaan Teknologi *Near Field Communication* Pada Telepon Seluler Untuk *Micro Payment* dan *Loyalty Management*.jurnal Konsultan Teknologi Informasi 3355-4453