BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan perkembangan internet dan kemudahan dalam pengaksesannya telah memberikan banyak pengaruh dalam kehidupan manusia. Jangkauan internet yang sangat luas dan bersifat global mempermudah menyebarkan informasi dan menjalin komunikasi antar penggunanya.Tidak sedikit pengguna internet memanfaatkan fasilitas ini untuk berjualan barang, berinteraksi sosial dengan pengguna lain, mempromosikan barang dan lain sebagainya (Pribadi, 2009). Hal ini tentu telah merubah paradigma perdagangan dimana aktivitas bisnisnya dapat dilakukan dimana saja dan kapan saja selama terhubung dengan internet yang dikenal dengan transaksi *online*.

Kagiatan transaksi *online* melalui media internet membutuhkan perputaran uang yang cepat dan terkontrol. Dengan demikian, penggunaan uang tunai dalam transaksi menjadi tidak efektif dan efisien.Untuk itu dikembangkan pemakaian cek dan kartu kredit sehingga transaksi bisa dilakukan dengan cepat, aman, dan dalam nominal yang besar (Sukariningrum, dkk. 2006). Namun menurut Tn, pada situs indocracker.wetpaint.com (Arsyad,2009, h.3) dalam bertransaksi *online*

menggunakan kartu kredit, umumnya data kartu kredit tersebut tersimpan dalam *database vendor/ merchant*, tentunya ini menjadi hal yang perlu untuk diperhatikan mengenai keamanan data privasi *customer* yang tersimpan pada *database* tersebut, banyak dari beberapa *hacker/cracker* mengklaim telah berhasil membobol *database* elektronik *wallet* seperti *paypal* misalnya dan mencuri akun kartu kredit *customer* di berbagai negara. Selain itu, pihak yang berwenang dapat mengetahui secara rinci, transaksi pembelian yang dilakukan pengguna.

Berbeda dengan kartu kredit, pembayaran dengan uang tunai menjaga anonimitas pengguna. Saat melakukan transaksi pembelian, tidak dapat diketahui identitas pembeli. Setelah melakukan transaksi, tidak dapat diketahui siapa pembelinya. Sulit untuk mengetahui rincian transaksi yang dilakukan pengguna berdasarkan nomor seri uang yang dipakai. Namun uang tunai memiliki kekurangan yaitu mudah dicuri orang lain dan tidak bisa digunakan dalam pembayaran transaksi *online*. Salah satu solusi masalah ini adalah dengan menggunakan uang digital (*digital cash).*

Transaksi *digital cash* merupakan transaksi elektronik yang menawarkan *property anonymous* dalam transaksinya untuk lebih menjaga privasi *customer* seperti pada transaksi konvensional menggunakan uang kertas (Arsyad,2009, h.4). *Property anonymous* atau *property privacy* ini merupakan pembedaan antara metode pembayaran *digital cash* dengan metode pembayaran lainnya. Untuk itu diperlukan

suatu cara untuk melindungi identitas *customer* atas penggunaan *digital cash*. *Property* ini harus mampu melindungi privasi *customer* baik dari *vendor* maupun dari bank yang mengeluarkan *digital cash. Blind signature* merupakan cara yang tepat untuk mengatasi masalah ini, dengan menerapkan konsep ini privasi *customer* dalam menggunakan *digital cash* dapat terlindungi.

1.2 Rumusan Masalah

Sesuai dengan latar belakang masalah di atas, dapat dirumuskan masalah yang harus di jawab dalam penelitian ini adalah:

1. Bagaiman cara menerapkan *blind signature* pada *digital cash*?
2. Bagaimana melindungi privasi *customer* dari bank dan dari *vendor* saat menggunakan *digital cash*?
3. Bagaimana membuktikan keaslian *digital cash* saat transaksi pembayaran?
4. Bagaimana menjaga keamanan *digital cash* yang dihasilkan?

1.3 Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut :

1. Skema *blind signature* yang digunakan dalam penelitian ini adalah *Chaum's Blind Signature protocol* yang diperkenalkan oleh David Chaum menggunakan algoritma RSA.
2. Protokol *digital cash* yang digunakan adalah protokol *online*. Dimana, proses validasi *digital cash* memerlukan autentikasi dari bank secara langsung.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan dari penelitian ini adalah sebagai berikut:

1. Mengimplementasikan *blind signature* dengan menggunakan algoritma RSA pada *digital cash*.
2. Membangun sistem yang mampu menghasilkan *digital cash* yang memenuhi syarat *property anonimity digital cash.*
3. Menghasilkan *digital cash* yang valid dalam transaksi pembayaran.
4. Membuat skema sistem yang mampu menjaga keamanan penggunaan *digital cash*.

1.5 Manfaat Penelitian

Beberapa manfaat yang dapat diperoleh dari penelitian yang dilakukan adalah sebagai berikut:

1. Mengetahui cara kerja pengamanan data dengan menggunakan algoritma RSA.
2. Mengetahui manfaat *blind signature* serta penerapannya dalam transaksi *digital cash*.
3. Hasil penelitian ini dapat digunakan sebagai rujukan untuk membangun sistem sistem pembayaran *online* yang lebih tangguh lagi.

1.6 Sistematika Penulisan

Pembahasan materi dalam penulisan ini terdiri dari 5 bab dan halaman lampiran secara terurut, yaitu:

BAB I PENDAHULUAN

Bab ini berisi latar belakang penelitian, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bagian ini memuat landasan teori yang berfungsi sebagai sumber atau alat dalam memahami permasalahan yang berkaitan dengan transaksi *online*, pembayaran *online*, *digital cash*, algoritma RSA ,*digital signature*, *dan blind signature.*

BAB III METODOLOGI PENELITIAN

Pada bab ini dijelaskan secara umum tahapan penlitian yang dilakukan, model proses yang digunakan, serta alat dan bahan yang digunakan selama penelitan berlangsung

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini berisi penjabaran hasil penelitian secara mendalam yang akan menjawab apa yang sudah dirumuskan dalam rumusan masalah.

BAB V KESIMPULAN DAN SARAN

Kesimpulan merupakan jawaban atas rumusan masalah, tujuan penelitian dan merupakan intisari dari BAB IV. Saran berisikan rekomendasi pengembangan sistem lebih lanjut.