BAB I

PENDAHULUAN

1.1 Latar Belakang

Penggunaan internet di seluruh dunia telah mencapai 31,7 miliar dan setiap tahunnya tumbuh hingga mencapai 7,6 % (Sherlyanita & Rakhmawati, 2016). Transaksi online sudah menjadi sangat umum dalam kehidupan sehari-hari yang memudahkan pengguna untuk melakukan transaksi lebih cepat dan aman (Khairnar & Kharat, 2016). Salah satu transaksi online yang perkembangannya cukup pesat adalah *electronic commerce*. *Electronic commerce* atau sering disebut *e-commerce* juga banyak dimanfaatkan oleh masyarakat yang ingin memperkenalkan, menawarkan serta melakukan proses transaksi online. *E-commerce* saat ini yang mulai berkembang dengan pesat di Indonesia adalah dengan munculnya transaksi secara online yaitu seperti dompetku, iPaymu, PayPal, Q-Pay dll (Putra, Dantes, & Candiasa, 2018). Berdasarkan hasil survey pada tahun 2014 apple pay merupakan salah satu produk yang dikeluarkan oleh payment gateway diperkenalkan produk ini memiliki antena NFC yang terpasang didalamnya untuk berkomunikasi dengan POS, apple menggunakan pemindai sidik jari untuk mengotentikasi pengguna untuk mengamankan informasi dalam suatu aplikasi, pada tahun 2015 mengenai *Costumer Digital Payment* ditemukan bahwa 16% pengguna lebih menyukai pembayaran secara digital, dimana 67% pengguna masih lebih memilih uang tunai (Ghosh, Goswami, Majumder, Kumar, & Mohanty, 2017).

Munculnya transaksi online dengan berbagai fitur yang ada, masih memunculkan polemik seputar masalah keamanan dalam bertransaksi secara online. Di satu sisi transaksi online memberikan kemudahan dalam melakukan transaksi, namun di sisi lain ditemukan terdapat beberapa contoh pembobolan data transaksi online salah satu contohnya yaitu kasus pembobolan akun lazada, proses transaksi yang dilakukan melalui pembayaran kartu kredit yang secara mudah dapat di retas (www.liputan6.com, 2016). Akibat kasus yang menimpanya kini

lazada, menerapkan sistem *two step verification* atau verifikasi ganda. Verifikasi ini dilakukan dengan dua cara yaitu verifikasi pertama melalui email dari lazada, sedangkan yang terverifikasi yang kedua melalui sms ke nomor nasabah yang terdaftar dibank penerbit kartu kredit untuk mencegah adanya pencurian data transaksi (Aldrin, 2017).

Secara umum algoritma yang banyak digunakan untuk mengamankan data transaksi digital yaitu algoritma kriptografi SHA-256 (*Secure Hash Algorithm*) (Yuricha, Tursina, & Nasution, 2017). Salah satu contoh sistem transaksi online yang menggunakan algoritma SHA-256 yaitu *blockchain* atau *bitcoin* (Fahmy, 2018). Kelebihan *bitcoin* adalah setiap proses transaksi yang dilakukan oleh *bitcoin* data yang tersimpan akan di enkripsi secara otomatis sehingga para hacker tidak bisa membobol data transaksi tersebut. Selain *bitcoin, Q-Pay* merupakan salah satu contoh aplikasi *mobile* berbasis android yang memiliki fungsi untuk melakukan pencatatan informasi dan transaksi pembelian pada aplikasi toko serta memilki fungsi sebagai alat pembayaran pada aplikasi konsumen. Dengan menggunakan aplikasi *Zxing* (*Zebra Crossing*) sebagai pemindai dan melakukan generalisasi data menjadi sebuah *QR Code.* Pada fitur keamanan data, Q-Pay menerapkan metode enkripsi AES-256 dengan memodifikasi enkripsi bertingkat (*Triple AES*). Modifikasi ini dilakukan agar terhindar dari adanya upaya pencurian data transaksi (Anshori, H, Samopa, & Suryotrisongko, 2013).

Selain algoritma SHA-256 dan AES-256, sebenarnya terdapat algoritma lain yang berpeluang untuk digunakan dalam pengamanan data transaksi digital, yaitu algoritma whirlpool. Algoritma whirlpool adalah salah satu fungsi hash satu arah. Whirlpool menerima masukkan suatu pesan berupa string dengan panjang maksimum 2^{256} bit, dan menghasilkan keluaran sebuah *message digest* dengan panjang tetap, yaitu 512 bit atau 128 angka dalam heksadesimal (Kitsos & Koufopavlou, 2004). Kelebihan dari algoritma whirlpool memiliki tingkat keamanan yang tinggi karena round *transformations* dapat diimplementasikan hanya dengan manipulasi dari delapan tabel difusi, whirlpool dapat menghasilkan message digest dengan waktu yang cukup cepat.

Kehadiran sistem pembayaran qr payment akan terus berkembang dengan pesat di indonesia, salah satunya sistem pembayaran dengan teknologi qr code

(quick response code) atau qr payment yang akan menjadi proses pembayaran utama dalam sebuah transaksi karena penggunaan qr payment lebih efektif dan efisien. Penggunaan qr payment di indonesia masih bersifat khusus, artinya hanya untuk aplikasi penerbit uang elektronik dan merchants tertentu saja yang sudah berkerjasama dan memiliki fasilitas layanan qr code yang bisa dilakukan pembayaran dengan pemindaian kode ini. Dengan kata lain penggunaan qr payment di indonesia belum open system. Sebagai contoh, pemindai yang ada pada aplikasi sakuku ataupun t-cash dan lainnya hanya bisa digunakan untuk membayar dengan qr code pada merchants yang sudah berkerjasama. Selain itu juga teknologi qr code ini awalnya digunakan kalangan industri manufaktur untuk melakukan inventarisir barang-barang produksinya. Namun lambat laun mulai bergeser ke fungsi-fungsi lainnya. Jika diperhatikan, sistem memindai kode batang (barcode scanning) selama ini sudah kerap digunakan untuk menandai produk-produk yang dijual di pasar modern, seperti minimarket, supermarket, toserba, dan lainnya. Barcode tersebut berisi sejumlah informasi mulai dari jenis atau nama produk beserta harganya. Sehingga memudahkan kasir menghitung jumlah belanjaan (okezone.com, 2018).

Selain itu juga, *QR Code* sangat cepat dalam mencapai tingkat keamanan yang tinggi. Semakin banyak orang yang menggunakan dan mengadopsi teknologi ini setiap harinya, Salah satu alasan dibalik cepatnya perkembangan *QR Code* adalah mendapat momentum ketika pengguna *smartphone* meningkat di seluruh dunia dan pemasar menggunakan *QR Code* untuk menjangkau konsumen seluler. (Dey, Uddin, Kabir, & Rahman, 2017). Selain itu juga *QR Code* memiliki kapasitas tinggi dalam data pengkodean yaitu mampu menyimpan semua jenis data seperti data numerik, data alphabet dan kode biner. Secara spesifik *QR Code* mampu menyimpan data jenis numerik sampai dengan 7.089 karakter, *QR Code* memiliki tampilan yang lebih kecil dari pada *barcode* ,hal ini dikarenakan *QR Code* mampu menampung data secara horizontal dan vertikal, oleh karena itu secara otomatis ukuran dari tampilan gambar *QR Code* bisa hanya sepersepuluh dari ukuran sebuah *barcode*. Tidak hanya itu *QR Code* juga tahan terhadap kerusakan, sebab *QR Code* mampu memperbaiki kesalahan sampai dengan 30%.

Pada tahun 2018 penggunaan sidik jari untuk keamanan dalam sebuah aplikasi meningkat lebih banyak, hal ini dikarenakan penggunaan fitur fingerprint dari sebuah aplikasi menjanjikan suatu tingkat keamaanan. Namun dengan demikian penggunaan fingerprint sudah banyak digunakan bahkan hingga sampai saat ini teknologi terbaru yang dikeluarkan oleh sebuah smartphone yaitu vivo 11 pro yang telah menggunakan screen touch ID yang hampir mirip dengan fingerprint, pada fitur keamanan screen touch id ini hadir sebagai revolusioner teknologi yang dimiliki oleh screen touch id, teknologi ini menjadi smartphone pertama di indonesia yang menerapkan fitur pengenalan sidik jari pada layar sentuh, screen touch id memiliki sensor sidik jari yang dapat mengidentifikasi sidik jari secara akurat dan tentu saja dapat dipastikan tingkat keamananya.

Berdasarkan permasalahan yang telah diuraikan, maka penelitian ini bertujuan untuk mengamanankan data transaksi dengan menggunakan *QR Code* sebagai pemindai data transaksi dan mengimplementasikan fungsi *hash* whirlpool sebagai keamanan data transaksi.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang yang telah dijelaskan, dapat dirumuskan permasalahan pada penelitian ini adalah sebagai berikut :

1. Bagaimana desain implementasi algoritma whirlpool dalam mengamankan data transaksi digital ?
2. Bagaimana integrasi *QR-Code, fingerprint* dalam mendukung algoritma whirlpool pada sistem keamanan transaksi digital ?
3. Bagaimana keandalan sistem keamanan transaksi digital yang terimplementasi algoritma whirlpool ?

1.3 Tujuan

Berikut adalah beberapa tujuan yang ingin dicapai dalam penelitian ini :

1. Mengembangkan sistem keamanan transaksi digital dengan menggunakan metode algoritma whirlpool
2. Mengimplementasikan *QR Code, fingerprint* sebagai generalisasi dalam bertransaksi

3. Melakukan pengujian keamanan aplikasi sistem keamanan transaksi digital yang sudah dibuat menggunakan *Man-in-the-Middle-Attact.*

1.4 Batasan Masalah

Terdapat beberapa batasan masalah dari penelitian ini, adalah :

1. Kode otentikasi berbasis heksadesimal
2. Penelitian dilakukan untuk melakukan analisis keamanan dari algoritma whirlpool
3. Pengujian keamanan aplikasi dengan menggunakan *Man-in-the-Middle Attack*
4. Hasil scanning *fingerprint* masih dalam bentuk citra digital
5. Data yang digunakan adalah data dummy
6. Pembagian blok pesan hanya menggunakan penguatan Merkle-Damgard dan Migayuchi Preneel
7. Sistem transaksi digital yang digunakan adalah e-money

1.5 Sistematika Penulisan

Berikut ini adalah sistematika penulisan yang dilakukan dalam menyusun skripsi :

BAB 1 PENDAHULUAN

Bab ini berisikan masalah yang diangkat dalam penelitian meliputi latar belakang (menceritakan tentang transaksi online secara umum, tentang kemanan dalam bertransaksi secara online, dan whirlpool sebagai metode atau algoritma untuk mengatasi masalah keamanan dalam bertransaksi), rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

BAB 2 KAJIAN TEORI

Berisi tentang kajian teori yang digunakan dalam penelitian meliputi teori tentang *Sistem Transaksi Digital, Kriptografi, Algoritma Whirlpool, QR Code, dan Fingerprint.*

BAB 3 METODOLOGI PENELITIAN

Berisikan dasar teori mengenai metodologi yang digunakan dalam melakukan penelitian meliputi desain rancangan penelitian, subjek penelitian, alat dan bahan penelitian.

BAB 4 HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi tentang hasil implementasi dari penelitian yang dilakukan, hasil penelitian terdiri dari mengamankan data transaksi, mengimplementasikan algoritma whirlpool dan menguji keandalan media transaksi online.

BAB 5 KESIMPULAN DAN SARAN

Berisi kesimpulan dan saran berdasarkan penelitian yang dilakukan dari mulai perumusan masalah hingga selesai.