

BAB 1

USULAN GAGASAN

1.1 Deskripsi Umum Masalah

1.1.1 Latar Belakang Masalah

Perkembangan Teknologi yang semakin canggih, membuat transaksi semakin mudah dan efektif untuk melakukan transaksi. Banyak cara dilakukan untuk melakukan transaksi, salah satunya dengan bertransaksi menggunakan *QR Code*. *QR Code* adalah sistem pembayaran tanpa uang maupun kartu yang cara kerjanya adalah dengan *scanning* kode. Selain bertransaksi *QR Code* juga digunakan untuk membuka formulir, memindahkan kontak telepon, menambahkan akun sosial media menjadi teman, dan juga untuk melakukaklemn presensi saat sekolah ataupun kuliah, maka dari itu *QR Code* sangat membantu pekerjaan manusia. Namun, semakin canggih dunia digital tentu memiliki kelemahan tersendiri seperti penipuan transaksi keuangan, mengganti *QR Code* palsu, dan pencurian data. Salah satu kasus yang terjadi yaitu kasus QRIS palsu di Masjid. Kasus penipuan dengan modus menggantikan QRIS kotak amal di Masjid Nurul Iman Blok M Square, Jakarta Selatan oleh seorang Pria. Kejadian tersebut terekam kamera CCTV Masjid. Setelah di tindak lanjuti, Polisi mengatakan bahwa kasus penempelan kode QRIS itu sudah tersebar di beberapa Masjid wilayah Jakarta Selatan [16].

Dengan begitu, penulis merancang untuk mengamankan transaksi *QR Code* menggunakan *Digital Signature*. *Digital Signature* atau *Digital Signature Scheme* adalah skema matematika untuk menunjukkan keaslian pesan atau laporan digital. *Digital Signature* yang valid menawarkan penerima alasan untuk menyetujui bahwa pesan dibuat dengan menggunakan pengirim yang diakui, dan bahwa itu berubah menjadi tidak berubah dalam transit. *Digital Signature* biasanya digunakan untuk distribusi perangkat lunak, transaksi keuangan, dan dalam kasus lain di mana sangat penting untuk menemukan palsu atau manipulasi [2].

Adapun aspek-aspek yang harus dipenuhi dalam keamanan informasi yaitu *confidentiality*, *integrity*, dan *availability*. Transaksi *QR Code* harus memenuhi aspek tersebut terutama dalam hal data *integrity*, artinya transaksi harus terjaga integritas datanya dari upaya perubahan yang dilakukan oleh pihak yang tidak berwenang, dan diakui keasliannya tanpa ada penyangkalan. sehingga diperlukan *Digital Signature* untuk melindungi kegiatan transaksi *QR Code*.

1.1.2 Tujuan Capstone

Adapun tujuan capstone terkait perlindungan transaksi *QR Code* diantaranya memastikan keaslian data pada *QR Code* dan mengidentifikasi sejauh mana *Digital Signature* dapat dilakukan untuk memverifikasi keaslian pengirim data dalam transaksi *QR Code*, sehingga data tidak dimanipulasi oleh pihak yang tidak sah.

1.1.3 Analisis Masalah

Penyalahgunaan *QR Code* dilakukan oleh oknum yang tidak bertanggung jawab dengan menyebarkan *QR Code* palsu. Keamanan dan integritas dari platform *QR Code* belum terjamin aman. Hal tersebut berdampak pada masyarakat terutama pengguna *QR Code*, mereka meragukan *QR Code* sebagai alat pembayaran. Untuk menghindari masalah keamanan transaksi pada *QR Code*, tentu harus diikuti dengan memberikan keamanan yang cukup untuk pengguna *QR Code* khususnya pelaku bisnis.

1.1.3.1 Aspek Ekonomi

Pesatnya perkembangan industri digital membuat *QR Code* ditemukan di berbagai tempat, salah satunya di kawasan yang banyak melakukan transaksi pembayaran. Hal ini memudahkan orang-orang untuk melakukan pembayaran tanpa harus membawa uang. Namun dengan banyaknya orang yang menggunakan *QR Code*, menjadikan kesempatan para oknum kejahatan digital untuk mendapatkan keuntungan secara pribadi dengan mengubah data *QR Code*. Hal ini menimbulkan kerugian finansial dan kepercayaan bagi para usaha terutama pengguna *QR Code*.

1.1.3.2 Aspek Teknologi

Pada aspek teknologi, *QR Code* palsu menyebabkan data dari *QR Code* tidak sesuai dengan pemilik *QR Code*. Adapun masalah yang terjadi pada *QR Code* adalah gangguan layanan, pengubahan, dan pencurian data dari *database*. Hal ini menyebabkan transaksi yang dilakukan berbeda dengan tujuan awal *QR Code* menjadi *QR Code* yang datanya telah dimanipulasi.

1.1.3.3 Aspek Sosial

Kesadaran masyarakat mengenai potensi penipuan terkait dengan *QR Code* sangat penting. Namun, sosialisasi kepada masyarakat adanya *QR Code* palsu sangat kurang. Dengan demikian, menyebabkan banyak pengguna *QR Code* yang tidak mengetahui apa yang terjadi pada data *QR Code* yang digunakan.

1.2 Analisa Solusi yang Ada

QR Code adalah image berupa matriks dua dimensi yang memiliki kemampuan untuk menyimpan data didalamnya. *QR Code* merupakan evolusi dari kode batang (*barcode*). *QR Code* sering digunakan untuk pembayaran digital, karena dapat dengan mudah dibaca oleh kamera ponsel pintar. Namun *QR Code* juga rentan terhadap serangan seperti pemalsuan dan pencurian data. Solusi perlindungan transaksi terhadap *QR Code* menggunakan *Digital Signature* dapat meningkatkan keamanan transaksi. *Digital Signature* digunakan untuk memastikan bahwa data *QR Code* asli dan tidak diubah. Steganografi digunakan untuk menyembunyikan data sensitif, seperti nomor kredit, dalam data *QR Code*.

Digital Signature adalah jenis tanda tangan yang menggunakan pin atau algoritma matematika untuk menandatangani dan memvalidasi keaslian suatu dokumen elektronik, file, atau perangkat lunak. Sehingga file yang dikirim secara digital bisa sampai ke penerima yang dituju dalam format asli tanpa perubahan sedikitpun [3]. *Digital Signature* menggunakan fungsi *hashing* kriptografi dan kriptografi asimetris untuk menandatangani data. Tanda tangan digital juga menyediakan autentikasi asal (atribusi ke individu tertentu), integritas data (bukti tertentu), integritas data (bukti bahwa data belum dirusak dalam perjalanan atau sebaliknya), dan non-repudiasi penanda tangan (penanda tangan tidak dapat menyangkal bahwa mereka menandatangani data) [4].

Tanda tangan digital ini kemudian dapat untuk memverifikasi keaslian dan integritas data. Dalam konteks *QR Code*, *Digital Signature* dapat digunakan untuk memastikan bahwa data *QR Code* asli dan tidak diubah. *QR Code* yang asli akan memiliki tanda tangan digital yang valid. Tanda tangan digital ini dapat diverifikasi menggunakan algoritma kriptografi yang sama digunakan untuk menghasilkannya.

1.3 Kesimpulan

Pada penelitian ini, penulis menggunakan *Digital Signature* sebagai meningkatkan keamanan transaksi terhadap *QR Code*. Hal ini *Digital Signature* dapat digunakan untuk memastikan bahwa data *QR Code* asli dan tidak diubah. Terdapat tiga aspek yang harus dipenuhi dalam keamanan informasi yaitu *confidentiality*, *integrity*, dan *availability*. Dengan demikian, masalah keamanan data pada *QR Code* dapat diatasi dengan solusi-solusi tersebut, sehingga dapat mengurangi aktivitas penipuan dengan mudah dan efektif. Dengan demikian, penulis merancang untuk mengamankan transaksi *QR Code* menggunakan *Digital Signature*.