PEMANFAATAN TEKNOLOGI DYNAMIC SECURE QR CODE UNTUK MENINGKATKAN VALIDITAS DAN KEAMANAN TRANSAKSI E-TICKET

Proposal Tugas Akhir

Oleh

Fahreza Yunanda
18221013

PROGRAM STUDI SISTEM DAN TEKNOLOGI INFORMASI
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG

Desember 2025

LEMBAR PENGESAHAN

PEMANFAATAN TEKNOLOGI DYNAMIC SECURE QR CODE UNTUK MENINGKATKAN VALIDITAS DAN KEAMANAN TRANSAKSI E-TICKET

Proposal Tugas Akhir

Oleh

Fahreza Yunanda
18221013

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Proposal Tugas Akhir ini telah disetujui dan disahkan
di Bandung, pada tanggal 17 Desember 2025

Pembimbing

Dr. Yusuf Kurniawan S.T., M.T.

NIP. 197203262008011014

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

I.1 Latar Belakang

Berdasarkan Kamus Besar Bahasa Indonesia (KBBI), Tiket atau karcis adalah surat kecil (carik kertas khusus) sebagai tanda telah membayar ongkos dan sebagainya (untuk naik bus, menonton bioskop, dan sebagainya). Tiket merupakan sebuah dokumen yang berfungsi sebagai bukti hak akses atau tanda pembayaran yang sah untuk menggunakan suatu layanan atau memasuki suatu area tertentu. Secara historis, tiket konvensional dalam bentuk fisik telah menjadi bagian tak terpisahkan dari berbagai sektor, mulai dari transportasi hingga hiburan. Namun, seiring dengan pesatnya perkembangan teknologi informasi, terjadi pergeseran paradigma menuju digitalisasi tiket menjadi tiket elektronik (*e-ticket*). Inovasi layanan ini sangat erat kaitannya dengan adopsi sistem teknis berbasis komputer yang memungkinkan peningkatan efisiensi dan efektivitas operasional (Lübeck dkk. 2012). Pergeseran paradigma tersebut didorong oleh kebutuhan untuk meningkatkan manajemen informasi yang sebelumnya sulit dilakukan dengan sistem manual atau kartu magnetik (Lübeck dkk. 2012).

Adopsi *e-ticket* mulai marak pada awal tahun 2000-an, yang dipelopori oleh industri penerbangan di tahun 1990-an, dan kini telah diadopsi secara masif di berbagai sektor. *E-ticket* menawarkan berbagai keunggulan signifikan dibandingkan tiket konvensional yang rentan terhadap inefisiensi. Lübeck dkk. (2012) menyoroti bahwa sistem konvensional seringkali terkendala oleh lemahnya kontrol operasional yang menyebabkan maraknya perdagangan tiket ilegal serta penyalahgunaan manfaat tiket khusus (seperti tiket pelajar) karena sulitnya identifikasi pengguna. Dari sisi pengguna, *e-ticket* memberikan kemudahan distribusi dan akses, menghilangkan risiko kehilangan tiket fisik, serta membantu menghindari antrean panjang. Selain itu, sistem ini juga lebih efisien dari segi biaya operasional karena mengurangi penggu-

naan kertas dan menghindari komisi yang dibayarkan kepada sistem distribusi dan agen.(Chen 2007).

Untuk merealisasikan berbagai keunggulan *e-ticket* tersebut, diperlukan medium representasi data yang efisien dan kompatibel dengan perangkat pengguna. Di antara berbagai alternatif teknologi, *Quick Response Code* (QR Code) muncul sebagai solusi dominan yang diadopsi secara luas dalam implementasi *e-ticket*. QR Code adalah jenis kode batang (*barcode*) matriks atau kode dua dimensi yang dapat menyimpan informasi digital (Shin dkk. 2012). Tidak seperti *barcode* satu dimensi, QR Code mengenkode data secara horizontal dan vertikal, menawarkan kepadatan informasi yang lebih tinggi dan kecepatan pembacaan yang lebih cepat (Alsuhibany 2025). Tiwari (2016) menjelaskan bahwa tingkat penerimaan QR Code yang tinggi secara global berbanding lurus dengan pertumbuhan pengguna ponsel pintar, yang memungkinkan teknologi ini menjangkau konsumen secara luas dan cepat. Ubikuitas perangkat pemindai yang terintegrasi dalam ponsel pintar, menjadikan QR Code pilihan yang praktis dan efisien untuk diterapkan sebagai medium *e-ticket*. Kepopuleran dan kemudahan akses tersebut mendorong adopsi luas QR Code pada gerbang transportasi maupun acara hiburan. Akan tetapi, di balik kenyamanan tersebut, model *e-ticket* konvensional yang mengandalkan QR Code dalam bentuk statis, secara inheren mewarisi celah keamanan yang serius.

Sistem *e-ticket* pada umumnya mengadopsi model kode QR statis. Pada model ini, data tiket seperti identitas pengguna atau tautan validasi, dienkode secara langsung ke dalam pola matriks citra. Karakteristik fundamental dari kode QR statis adalah informasi yang tersimpan di dalamnya bersifat tetap (*fixed information*) (Yanuarafi 2023); artinya, setelah kode dibangkitkan (*generated*), pola visualnya tidak akan berubah dan terus valid sepanjang masa berlaku tiket. Proses validasi bergantung sepenuhnya pada pemindaian di pintu masuk, yaitu saat alat pemindai menerjemahkan kembali pola matriks menjadi data identitas untuk dicocokkan dengan basis data. Meskipun arsitektur ini menawarkan kemudahan implementasi, menurut Yanuarafi (2023), penggunaan kode QR statis memiliki kelemahan signifikan dalam aspek keamanan. Sifatnya yang permanen membuat sistem ini rentan terhadap penyalahgunaan, seperti duplikasi ilegal dan pemalsuan, yang pada akhirnya mengancam integritas ekosistem *e-ticket* secara keseluruhan.

Kelemahan mendasar dari arsitektur statis adalah sifatnya yang “sekali terbit, berlaku selamanya” tanpa mekanisme pembaruan autentikasi. Celah tersebut dieksploitasi secara luas melalui serangan penggandaan (*cloning*) dan serangan putar ulang

(*replay attack*). Sung dkk. (2015) dalam analisis keamanannya menegaskan bahwa kode QR sangat mudah diduplikasi melalui fitur tangkapan layar (*screen capture*) pada perangkat seluler, yang kemudian dapat ditransfer ke pihak lain tanpa bisa dicegah oleh sistem konvensional. Dampak dari kerentanan ini menciptakan efek domino kerusakan pada ekosistem pertiketan.

Pertama, pada aspek validasi di lapangan, insiden konser Coldplay di Jakarta tahun 2023 memperlihatkan kekacauan di pintu masuk ketika banyak pemegang tiket sah gagal mendapatkan akses karena tiket mereka telah digandakan dan digunakan lebih dulu oleh pihak lain. Berdasarkan analisis hukum, modus ini terjadi karena pelaku mempelajari desain visual tiket statis lalu menggandakannya untuk dijual ke banyak korban (Berma 2023). Kedua, lemahnya sistem keamanan turut menyuburkan praktik percaloan (*scalping*), yaitu dengan menjual kembali tiket yang telah dibeli secara legal, dengan harga berkali-kali lipat dari harga resmi sehingga merusak kewajaran pasar (Pamela 2023). Ketiga, kegagalan kontrol akses berlanjut hingga ke dalam arena, seperti pada salah satu pertandingan Timnas Indonesia di GBK. Pada kasus tersebut, penonton tanpa hak akses valid berhasil masuk dan menduduki kursi pemegang tiket sah, memicu konflik fisik dan ketidaknyamanan (Kurniawan 2024). Terakhir, dari sisi kerugian materiil, investigasi Kompas mengungkapkan data Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) yang mencatat 182 kasus transaksi mencurigakan terkait penipuan tiket konser pada tahun 2024 dengan total nilai Rp 2,3 miliar (Diveranta dkk. 2025). Rangkaian kasus ini menegaskan bahwa sistem konvensional saat ini gagal memberikan perlindungan menyeluruh, baik dari sisi keamanan akses, keadilan harga, maupun perlindungan hak konsumen.

Kompleksitas permasalahan tersebut mulai dari kekacauan validasi fisik, inflasi harga akibat percaloan, hingga kerugian materiil akibat penipuan, membuktikan bahwa sistem verifikasi yang hanya mengandalkan kode QR statis tidak lagi memadai. Diperlukan sebuah pendekatan komprehensif untuk menjamin integritas transaksi dan data. Berdasarkan analisis masalah tersebut, sebuah *e-ticket* yang ideal harus memiliki tiga karakteristik pertahanan utama. Pertama, tiket harus bersifat dinamis (*dynamic*) menggunakan mekanisme pembangkitan kode QR yang berubah secara berkala berbasis waktu sehingga tangkapan layar menjadi tidak valid setelah durasi tertentu (Sung dkk. 2015). Kedua, tiket harus mengutamakan pelindungan privasi (*privacy preservation*) melalui penerapan prinsip minimalisasi data (*data minimization*). Hal ini dicapai dengan membatasi muatan data (*payload*) pada kode QR hanya untuk atribut teknis non-sensitif guna mencegah risiko eksfiltrasi data pribadi pengguna (*PII leak*) dari penyimpanan lokal. Ketiga, tiket harus bersifat aman (*secure*) meng-

gunakan mekanisme tanda tangan digital (*digital signature*) yang menjamin aspek nirsangkal (*non-repudiation*), untuk memastikan tiket diterbitkan oleh otoritas yang sah dan tidak dimodifikasi.

Namun, pengamanan data tiket hanyalah satu sisi dari solusi. Tantangan lain yang tak kalah penting dalam penyelenggaraan acara berskala besar adalah risiko operasional akibat ketergantungan penuh pada konektivitas internet, atau dikenal sebagai Titik Kegagalan Tunggal (*Single Point of Failure*). Arsitektur sistem konvensional yang mewajibkan setiap pemindaian tiket terhubung langsung ke server pusat sangat rentan lumpuh saat terjadi lonjakan beban trafik atau gangguan jaringan. Kerentanan ini terbukti dari insiden kendala teknis pada *platform* Ticketmaster saat penjualan tiket konser Taylor Swift, yang menunjukkan bahwa server pusat memiliki batas toleransi beban yang nyata dan dapat lumpuh seketika akibat lonjakan permintaan (Labs 2023). Risiko serupa juga mengintai infrastruktur awan (*cloud*). Laporan insiden Amazon Web Services (AWS) pada tahun 2017 memperlihatkan bagaimana kesalahan teknis pada satu layanan inti dapat menyebabkan kegagalan berantai pada sistem lain yang bergantung padanya (Amazon Web Services 2017). Jika server validasi tiket mengalami gangguan serupa saat acara berlangsung, alat pemindai di lokasi akan kehilangan fungsinya dan memicu kemacetan fatal di gerbang masuk.

Oleh karena itu, untuk menjamin keberlangsungan proses validasi di tengah ketidakpastian kondisi jaringan, diperlukan mekanisme validasi mandiri (*offline validation*) pada perangkat pemindai. Agar perangkat dapat memvalidasi tiket secara mandiri tanpa menghubungi server, diperlukan strategi manajemen *cache* lokal yang menyimpan kredensial validasi (seperti kunci publik dan daftar tiket) secara aman di sisi perangkat. Selanjutnya, karena validasi dilakukan secara lokal, tantangan berikutnya adalah bagaimana menyinkronkan status penggunaan tiket kembali ke server pusat tanpa membebani jaringan secara *real-time*. Untuk menjawab hal ini, diterapkan mekanisme sinkronisasi data asinkron atau *batching*, yaitu data log validasi dikirimkan secara berkala atau saat koneksi stabil sehingga integritas data terjaga tanpa mengorbankan kecepatan validasi di lapangan.

Dengan demikian, penelitian ini mengusulkan pengembangan sistem *Dynamic Secure QR Code* yang tidak hanya fokus pada aspek keamanan anti-percaloan melalui algoritma token dinamis, tetapi juga mengintegrasikan mekanisme validasi hibrida (kombinasi *online* dan *offline*). Melalui pemanfaatan *cache* lokal dan sinkronisasi *batching*, sistem ini diharapkan mampu menghadirkan solusi pertiketan yang aman dari pemalsuan dan tangguh (*resilient*) terhadap gangguan infrastruktur jaringan.

I.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, teridentifikasi adanya kelemahan fundamental pada arsitektur *e-ticket* berbasis Kode QR statis yang rentan terhadap berbagai eksploitasi keamanan. Oleh karena itu, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana merancang arsitektur sistem *e-ticket* berbasis token dinamis (*Dynamic Secure QR Code*) yang memiliki resistensi terhadap serangan penggandaan (*cloning*) dan *replay attack* dengan tetap mempertahankan aspek privasi pengguna?
2. Bagaimana mekanisme validasi tiket yang mampu menjamin ketersediaan layanan (*high availability*) dan mencegah kegagalan sistem (*Single Point of Failure*) meskipun terjadi gangguan pada infrastruktur jaringan server pusat?
3. Bagaimana menjaga konsistensi data status penggunaan tiket antara sisi klien dan server pusat agar integritas data tetap terjaga tanpa mengorbankan responsivitas waktu tunggu (*latency*) pada proses validasi di lapangan?

I.3 Tujuan Penelitian

Mengacu pada rumusan masalah di atas, tujuan utama dari penelitian ini adalah:

1. Merancang dan mengimplementasikan arsitektur sistem *e-ticket* berbasis token dinamis (*Dynamic Secure QR Code*) yang memanfaatkan algoritma pembangkitan kode berbasis waktu dan tanda tangan digital untuk menjamin keaslian tiket serta melindungi data pribadi pengguna.
2. Mengembangkan mekanisme validasi mandiri (*offline validation*) pada perangkat pemindai dengan memanfaatkan manajemen penyimpanan lokal (*local cache*), teknik derivasi kunci (*Key Derivation*), dan kriptografi kunci publik sehingga sistem tetap andal tanpa ketergantungan koneksi server terus-menerus.
3. Menerapkan mekanisme sinkronisasi data asinkron (*batching*) untuk menjamin integritas dan konsistensi data status tiket antara perangkat pemindai dan server pusat secara efisien tanpa membebani kinerja operasional di lapangan.

I.4 Batasan Masalah

Agar pengerjaan tugas akhir dapat lebih terarah dan tidak melenceng dari tujuan utamanya, ruang lingkup permasalahan dibatasi sebagai berikut:

1. Penelitian ini berfokus pada perancangan dan implementasi modul inti ke-

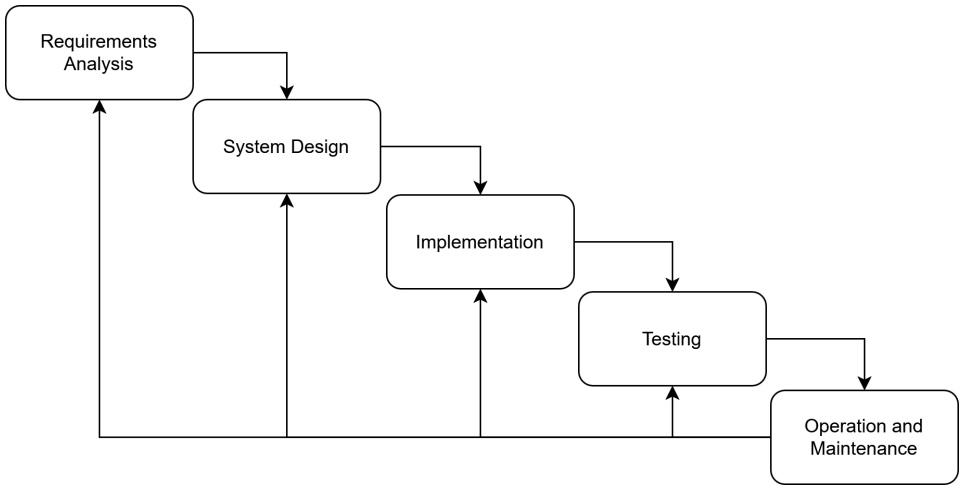
amanan, yaitu proses pembangkitan (*generation*) dan validasi (*validation*) *Dynamic Secure QR Code*, tanpa membahas aspek antarmuka pengguna (UI-/UX) secara mendalam.

2. Penelitian ini tidak mencakup pengembangan fitur sistem penjualan tiket yang kompleks (seperti manajemen akun pengguna, integrasi gerbang pembayaran, atau manajemen acara), melainkan fokus pada siklus hidup tiket mulai dari penerbitan hingga validasi.
3. Luaran sistem yang dibangun berupa prototipe (*proof-of-concept*) yang bertujuan untuk mendemonstrasikan kelayakan logika keamanan dan mekanisme *offline*, bukan sebagai aplikasi skala produksi yang siap rilis komersial.
4. Sistem menerapkan prinsip *Data Minimization*, yaitu muatan data (*payload*) pada Kode QR tidak dienkripsi, melainkan hanya berisi informasi non-sensitif (seperti ID referensi). Keamanan data sensitif pengguna diasumsikan terjamin pada basis data server pusat.
5. Implementasi teknis prototipe akan dikembangkan menggunakan teknologi perangkat lunak yang relevan dan mendukung pustaka (*library*) kriptografi standar, tanpa terikat pada satu bahasa pemrograman spesifik.
6. Penelitian tidak mencakup perancangan perangkat keras (*hardware*) pemindai khusus. Proses pemindaian dan validasi diasumsikan dilakukan menggunakan perangkat lunak pada ponsel pintar (*smartphone*) yang memanfaatkan kamera bawaan.
7. Perangkat pemindai diasumsikan sebagai perangkat terpercaya (*trusted device*) yang memiliki mekanisme keamanan fisik memadai. Risiko pencurian fisik perangkat pemindai dan teknik *reverse engineering* untuk mengekstrak kunci rahasia utama (*Master Secret*) dianggap sebagai risiko operasional di luar lingkup sistem yang dirancang.
8. Implementasi dan pengujian sistem diasumsikan menggunakan satu perangkat pemindai (*single gate scanner*) pada satu waktu. Isu sinkronisasi data secara *real-time* (*peer-to-peer*) antar-banyak pemindai dalam kondisi *offline* berada di luar lingkup penelitian ini.

I.5 Metodologi

Pengerjaan tugas akhir ini menerapkan kerangka kerja *Software Development Life Cycle* (SDLC) dengan pendekatan model *Waterfall* sebagai metodologi. Model ini dipilih karena pengerjaan tugas akhir yang memiliki kebutuhan sistem (*requirements*) yang didefinisikan secara jelas di tahap awal, yaitu berfokus pada aspek keamanan QR Code, serta membutuhkan alur pengerjaan yang terstruktur. Tahapan

pengembangan sistem dalam pengerjaan tugas akhir mengacu pada standar rekayasa perangkat lunak menurut Sommerville (2016), yang secara visual dapat dilihat pada Gambar I.1.



Gambar I.1 Alur Metodologi Penelitian Model Waterfall

Rincian tahapan yang akan dilalui selama pelaksanaan tugas akhir adalah sebagai berikut:

1. **Analisis Kebutuhan (*Requirements Analysis*)**
   Tahapan ini merupakan langkah fundamental untuk mengumpulkan fakta empiris dan merumuskan spesifikasi kebutuhan sistem. Proses investigasi dilakukan dengan mengobservasi fenomena kegagalan sistem *e-ticket* (*system crash*) pada acara berskala besar, serta mengumpulkan data sekunder dari sumber kredibel, seperti laporan PPATK dan pemberitaan media massa terkait modus kejahatan tiket. Selain itu, dilakukan studi literatur terhadap mekanisme *offline-first*, sinkronisasi data (*batching*), serta standar teknis kriptografi seperti *Time-based One-Time Password* (TOTP) dan Tanda Tangan Digital untuk menjawab permasalahan keamanan dan ketersediaan sistem.
2. **Perancangan Sistem (*System Design*)**
   Pada tahap ini, spesifikasi kebutuhan diterjemahkan menjadi representasi desain perangkat lunak yang mencakup tiga fokus utama. Pertama, dilakukan pemodelan arsitektur sistem hibrida yang menggambarkan interaksi antara server penerbit, penyimpanan lokal (*local cache*), dan perangkat pemindai. Kedua, dilakukan perancangan logika melalui diagram alur (*Flowchart*) untuk mendetailkan algoritma pembangkitan tiket, mekanisme validasi mandiri (*offline*), dan protokol sinkronisasi data asinkron. Terakhir, tahap ini meliputi perancangan antarmuka pengguna (*User Interface*) untuk memastikan fitur pemindaian dapat berjalan responsif.

3. **Implementasi (*Implementation*)**

   Tahapan ini bertujuan untuk merealisasikan rancangan desain menjadi unit program yang fungsional. Implementasi dilakukan dengan mengembangkan aplikasi seluler (*mobile app*) menggunakan teknologi yang relevan (seperti React Native/Expo) yang berfungsi sebagai dompet tiket dan alat pemindai. Logika keamanan inti akan diimplementasikan untuk menangani dua peran: (1) Sisi *Backend* untuk penandatanganan dan penerbitan tiket, dan (2) Sisi Perangkat Pemindai untuk melakukan dekripsi dan validasi tanda tangan digital secara lokal tanpa ketergantungan penuh pada koneksi server.

4. **Pengujian (*Testing*)**

   Setelah prototipe berhasil dibangun, tahap pengujian dilakukan untuk memverifikasi keandalan sistem. Pengujian mencakup dua skenario utama: (1) *Security Testing* untuk menguji ketahanan terhadap serangan tangkapan layar (*screenshot*) dan pemalsuan tiket; serta (2) *Availability Testing* untuk menguji kemampuan sistem melakukan validasi tiket dalam kondisi tanpa koneksi internet (*offline*) dan memastikan data tersinkronisasi dengan benar saat koneksi kembali tersedia (*batching*).

5. **Operasi dan Pemeliharaan (*Operation and Maintenance*)**

   Dalam konteks pengerjaan tugas akhir, tahapan ini diadaptasi menjadi fase dokumentasi dan penyusunan laporan. Pengerjaannya difokuskan pada penyusunan laporan akhir. Seluruh artefak tugas akhir, mulai dari hasil analisis, desain, kode program, hingga hasil pengujian keamanan dan ketersediaan, akan didokumentasikan secara sistematis. Tahapan ini juga mencakup penarikan kesimpulan untuk menjawab rumusan masalah serta saran perbaikan untuk pengembangan selanjutnya.

BAB II

STUDI LITERATUR

II.1 Sistem Tiket Elektronik (*E-Ticket*)

Perkembangan teknologi informasi telah mengubah paradigma layanan di berbagai sektor industri, termasuk dalam manajemen akses dan reservasi melalui sistem tiket elektronik atau *e-ticket*. Subbab ini akan membahas definisi, evolusi, serta karakteristik fundamental dari sistem *e-ticket*.

II.1.1 Definisi dan Konsep Dasar

Menurut Kamus Besar Bahasa Indonesia (KBBI), tiket atau karcis adalah surat kecil (carik kertas khusus) sebagai tanda telah membayar ongkos dan sebagainya (untuk naik bus, menonton bioskop, dan sebagainya). Tiket merupakan dokumen yang berfungsi sebagai hak akses atau tanda pembayaran yang sah untuk menggunakan suatu layanan. Seiring dengan perkembangan teknologi, terjadi transformasi bentuk tiket konvensional yang berbasis kertas menjadi wujud digital yang tersimpan dalam basis data komputer, yang disebut sebagai *electronic ticket* atau *e-ticket*.

Secara konseptual, *e-ticket* bukan sekadar penggantian media kertas, melainkan sebuah kontrak digital yang merepresentasikan hak kepemilikan atas suatu layanan atau produk. Informasi yang sebelumnya tercetak di atas kertas seperti detail acara, nomor kursi, dan identitas pemegang, kini dikodekan menjadi data digital yang dihubungkan dengan basis data di server pusat. Hal ini memungkinkan proses validasi dilakukan secara *real-time* melalui pencocokan data, bukan sekadar pemeriksaan visual fisik kertas.

II.1.2 Evolusi dan Transformasi Digital

Pergeseran menuju *e-ticket* merupakan bagian dari proses inovasi layanan yang lebih luas. Dalam konteks transportasi publik, Lübeck dkk. (2012) menjelaskan bah-

wa tiket elektronik dikembangkan sebagai evolusi dari sistem kartu pita magnetik dan tiket kertas konvensional. Pengembangan ini didorong oleh kekhawatiran akan inefisiensi dalam manajemen informasi dan kontrol operasi pada sistem terdahulu.

Pada fase awal, sistem konvensional seringkali terkendala oleh keterbatasan dalam pelacakan data. Adopsi sistem teknis terkomputerisasi kemudian muncul sebagai solusi untuk meningkatkan efisiensi dan efektivitas operasional. Menurut Lübeck dkk. (2012), implementasi sistem tiket elektronik merupakan bentuk inovasi proses yang merampingkan dan mengkualifikasi operasional dengan mengurangi proses manual sehingga meningkatkan kualitas layanan secara keseluruhan. Transformasi ini mengubah cara pengelolaan informasi karena sistem kini mampu meregistrasi pengguna, mengontrol penjualan kredit, dan menerbitkan laporan manajemen yang akurat untuk pemantauan data.

II.1.3 Keunggulan dan Efisiensi Operasional

Adopsi luas sistem *e-ticket* didorong oleh berbagai keunggulan signifikan dibandingkan sistem konvensional. Chen (2007) menyoroti bahwa motivasi utama maskapai penerbangan beralih ke *e-ticketing* adalah penghematan biaya distribusi tiket dan biaya penanganan (*handling overheads*). Sistem ini memungkinkan eliminasi tiket kertas, yang berdampak langsung pada pengurangan biaya tenaga kerja, pencetakan, pengiriman, dan akuntansi. Bagi pengguna, manfaat utamanya adalah kenyamanan akibat sifat tiket yang *paperless*, yang secara spesifik menghilangkan risiko kehilangan tiket fisik sebelum perjalanan.

Di sisi lain, dalam konteks transportasi darat, Lübeck dkk. (2012) menekankan bahwa keuntungan krusial dari *e-ticket* terletak pada peningkatan manajemen informasi dan kontrol. Sistem ini efektif membatasi perdagangan tiket ilegal (*illegal trade*) yang sebelumnya marak terjadi pada tiket fisik, serta mempersulit penyalahgunaan manfaat tiket khusus (seperti tiket pelajar) karena kredit tiket kini bersifat personal dan tidak dapat dipindahtangankan. Selain itu, sistem elektronik juga meningkatkan keamanan dengan mengurangi jumlah uang tunai yang beredar di dalam kendaraan, sehingga mengurangi daya tarik bagi tindak kejahatan seperti perampokan.

II.2 Teknologi *Quick Response* kode (QR)

II.2.1 Sejarah dan Prinsip Kerja

Quick Response Code (Kode QR) adalah jenis kode batang matriks dua dimensi yang dikembangkan oleh Denso Wave pada tahun 1994. Awalnya ditujukan untuk pelacakan inventaris suku cadang kendaraan, teknologi ini kini telah diadopsi secara masif di berbagai sektor mulai dari pemasaran hingga manajemen akses (Tiwari 2016; Shin dkk. 2012). Shin dkk. (2012) mendefinisikan kode QR sebagai pola persegi yang terdiri dari modul hitam dengan latar belakang putih yang dirancang untuk didekodekan dengan kecepatan tinggi menggunakan perangkat pemindai atau kamera ponsel pintar.

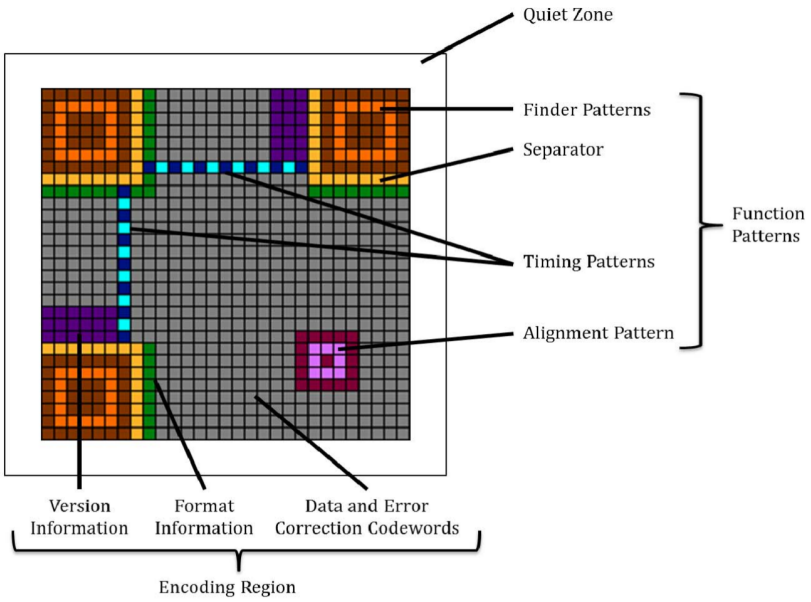
Berbeda dengan kode batang (*barcode*) satu dimensi yang hanya menyimpan data secara horizontal, kode QR mengodekan informasi dalam dua arah, yaitu vertikal dan horizontal. Struktur dua dimensi ini memungkinkan kode QR memiliki densitas informasi yang jauh lebih tinggi dan kapasitas penyimpanan yang lebih besar dalam ruang fisik yang lebih kecil dibandingkan pendahulunya (Alsuhibany 2025). Kapasitas ini memungkinkan penyimpanan berbagai jenis mode data, termasuk numerik, alfanumerik, biner, hingga karakter Kanji (Tiwari 2016), yang menjadikannya medium ideal untuk menyimpan data tiket elektronik yang kompleks.

II.2.2 Struktur Kode QR

Kemampuan kode QR untuk dibaca dengan cepat dan akurat (*high-speed reading*) didukung oleh strukturnya yang unik. Berdasarkan spesifikasi teknis yang dijelaskan oleh Tiwari (2016), setiap simbol kode QR dibangun dari modul-modul persegi yang disusun dalam *array* persegi reguler. Struktur ini terdiri dari dua bagian utama, yaitu pola fungsi (*function patterns*) dan wilayah pengodean (*encoding region*), yang dikelilingi oleh batas zona tenang (*quiet zone*) di keempat sisinya.

Wilayah pengodean (*encoding region*) berisi data yang merepresentasikan informasi versi, informasi format, data konten, dan *codeword* koreksi kesalahan. Sementara itu, pola fungsi adalah bentuk-bentuk spesifik yang ditempatkan di area tertentu untuk memastikan pemindai dapat mengidentifikasi dan mengorientasikan kode dengan benar. Terdapat empat jenis pola fungsi, yaitu *finder pattern*, *separator*, *timing patterns*, dan *alignment patterns*.

Komponen visual utama kode QR dapat dilihat pada Gambar II.1, dan untuk rincian dari *function patterns* dijelaskan sebagai berikut:



Gambar II.1 Struktur Kode QR (Tiwari 2016)

a) ***Finder Pattern*:** Tiga struktur kotak konsentris yang terletak di sudut kiri atas, kanan atas, dan kiri bawah. Pola ini memungkinkan pemindai mendeteksi posisi dan orientasi kode dari segala arah (360 derajat), sehingga pemindaian dapat dilakukan secara omni-direksional.
b) ***Separators*:** Area selebar satu modul berwarna putih (kosong) yang terletak di antara setiap *finder pattern* dan wilayah pengodean (*encoding region*) untuk memisahkan keduanya.
c) ***Alignment Pattern*:** Pola yang berfungsi mengoreksi distorsi jika kode dipindai pada permukaan melengkung atau sudut miring.
d) ***Timing Pattern*:** Garis putus-putus yang menghubungkan pola pencari untuk menentukan koordinat modul dan kepadatan simbol.
e) ***Quiet Zone*:** Area margin kosong di sekeliling simbol (minimal selebar 4 modul) yang memisahkan kode dari elemen visual di sekitarnya.

II.2.3 Koreksi Kesalahan (*Error Correction*)

Salah satu keunggulan teknis kode QR yang krusial untuk implementasi *e-ticket* adalah kemampuan koreksi kesalahan menggunakan algoritma Reed-Solomon. Fitur ini memungkinkan data tetap dapat dipulihkan dan dibaca meskipun sebagian area simbol rusak atau kotor (Tiwari 2016). Tingkat koreksi kesalahan dibagi menjadi empat level sebagaimana ditampilkan pada Tabel II.1.

Pemilihan level koreksi kesalahan ini menjadi pertukaran (*trade-off*) antara keta-

Tabel II.1 Tingkat Koreksi Kesalahan (*Error Correction Level*) pada kode QR (Tiwari 2016)

Level	Keterangan	Kemampuan Pemulihan Data
L	*Low* (Rendah)	$\approx 7\%$
M	*Medium* (Menengah)	$\approx 15\%$
Q	*Quartile* (Tinggi)	$\approx 25\%$
H	*High* (Sangat Tinggi)	$\approx 30\%$

hanan kode dan kapasitas data. Level M atau Q umumnya direkomendasikan untuk tiket elektronik yang berisiko mengalami kerusakan fisik (jika dicetak) atau gangguan tampilan layar (Tiwari 2016).

II.2.4 Kode QR Statis vs. Dinamis

Dalam implementasi sistem informasi, kode QR dikategorikan berdasarkan sifat data yang dikandungnya. Pemahaman terhadap perbedaan ini sangat penting dalam konteks keamanan tiket.

a) Kode QR Statis: Informasi dienkodekan secara langsung dan permanen ke dalam pola matriks. Sifatnya yang *fixed information* berarti data tidak dapat diubah setelah kode dibangkitkan. Yanuarafi (2023) mencatat bahwa jenis ini memiliki kelemahan keamanan karena pola visualnya yang tetap memudahkan pelaku kejahatan untuk melakukan duplikasi.

b) Kode QR Dinamis (Umum): Dalam definisi pemasaran umum, kode QR dinamis menyimpan sebuah tautan pendek (*short URL*) yang mengarahkan pengguna ke server tujuan. Pola QR tetap sama, namun konten di server bisa diubah. Meskipun fleksibel, pendekatan ini masih rentan terhadap penggandaan jika tautan tersebut tidak dilindungi mekanisme otentikasi tambahan.

c) Kode QR Dinamis Berbasis Waktu (Konteks Pengerjaan Tugas Akhir): Berbeda dengan definisi pada umumnya, pengerjaan tugas akhir ini mengadopsi konsep dinamis yang muatan data (*payload*) berubah secara periodik menggunakan algoritma berbasis waktu. Hal ini menyebabkan pola visual kode QR berubah total setiap interval waktu tertentu. Sung dkk. (2015) menyoroti pentingnya mekanisme kedaluwarsa (*expiration*) pada kode QR untuk mencegah penggunaan ulang kode yang telah disalin. Dengan pendekatan ini, salinan tiket hasil tangkapan layar (*screenshot*) akan menjadi tidak valid secara otomatis setelah durasi waktu tertentu habis.

II.3 Ancaman dan Kerentanan pada Sistem *E-Ticket*

Dalam konteks keamanan informasi, penting untuk membedakan antara ancaman (*threat*) dan serangan (*attack*). Ancaman merujuk pada potensi kejadian negatif yang dapat merugikan aset sistem, reputasi, atau nilai ekonomi penyedia layanan. Sementara itu, serangan adalah metode atau teknik spesifik yang dieksekusi oleh pelaku kejahatan untuk mengeksploitasi celah keamanan guna merealisasikan ancaman tersebut. Subbab ini akan menguraikan lanskap ancaman dari perspektif bisnis dan operasional, serta menganalisis vektor serangan teknis yang memungkinkan ancaman tersebut terjadi.

II.3.1 Identifikasi Ancaman (*Threat Landscape*)

Ancaman merepresentasikan risiko tingkat tinggi yang dihadapi oleh ekosistem pertiketan. Berdasarkan studi kasus dan literatur terkini, terdapat empat kategori ancaman utama yang menjadi fokus mitigasi:

a) Praktik Percaloan (*Scalping*): Calo atau makelar menurut Kamus Besar Bahasa Indonesia (KBBI) adalah orang yang menjadi perantara dan memberikan jasanya untuk menguruskan sesuatu berdasarkan upah. Ini adalah ancaman ekonomi yang terjadi ketika seseorang menjual kembali tiket yang dibelinya, namun dengan harga berkali-kali lipat dari harga normalnya yang merusak kewajaran pasar. Pamela (2023) melaporkan bahwa praktik ini sangat merugikan konsumen secara finansial dan merusak reputasi penyelenggara acara. Untuk memitigasi ancaman ini, diperlukan mekanisme validasi yang menjamin bahwa tiket yang ditampilkan adalah versi terbaru dan valid pada saat pemindaian, bukan salinan yang telah kedaluwarsa.

b) Penipuan Tiket (*Fraud*): Ancaman kriminal berupa penjualan tiket palsu atau tiket yang tidak valid kepada konsumen. Investigasi Diveranta dkk. (2025) mencatat kerugian miliaran rupiah akibat praktik ini, yang mengancam kepercayaan publik terhadap sistem penjualan tiket digital.

c) Infiltrasi Akses Ilegal: Ancaman operasional yang terjadi ketika individu tidak berhak berhasil memasuki area acara. Hal ini tidak hanya merugikan pendapatan, tetapi juga menimbulkan risiko keamanan fisik dan ketidaknyamanan bagi pemegang tiket sah yang kursinya ditempati pihak lain (Kurniawan 2024).

d) Ancaman Kegagalan Titik Tunggal (*Single Point of Failure*): Ancaman sistemik yang muncul ketika infrastruktur jaringan atau server pusat mengalami gangguan. Lever dkk. (2013) mendefinisikan *Single Point of Failure* (SPoF)

dalam sistem yang terintegrasi sebagai komponen kritis yang jika gagal, akan menyebabkan kegagalan operasional seluruh sistem karena terhambatnya transmisi data. Dalam konteks arsitektur server, Ghomi dkk. (2017) menegaskan bahwa ketergantungan pada *node* pengendali terpusat (*centralized*) menciptakan risiko SPoF yang tinggi; jika *node* pusat tersebut mengalami gangguan atau kelebihan beban (*overload*), maka seluruh layanan akan terhenti total. Hal ini sangat relevan dengan risiko kelumpuhan validasi tiket di gerbang masuk saat terjadi gangguan jaringan massal.

II.3.2 Analisis Vektor Serangan (*Attack Vectors*)

Untuk mewujudkan ancaman-ancaman di atas, pelaku kejahatan menggunakan berbagai metode serangan teknis yang mengeksploitasi kelemahan pada kode QR statis. Berikut adalah analisis mengenai metode serangan tersebut:

a) Serangan Penggandaan (*Cloning Attack*): Serangan ini merupakan metode utama untuk melakukan penipuan tiket. Pelaku menyalin citra kode QR yang sah melalui fitur tangkapan layar (*screen capture*) dan mendistribusikannya kepada korban. Sung dkk. (2015) menegaskan bahwa kerentanan utama sistem *mobile* adalah kemudahan menduplikasi tampilan layar, yang disebabkan oleh sistem statis yang gagal membedakan antara citra asli di aplikasi dan citra salinan di galeri foto.

b) Serangan Putar Ulang (*Replay Attack*): Serangan ini mengeksploitasi validitas data tiket yang tidak memiliki batasan waktu yang ketat. Dalam skenario ini, data tiket yang sah ditangkap (disalin) dan dikirimkan ulang (*replayed*) ke sistem pemindai di waktu atau lokasi berbeda. Tanpa mekanisme kedaluwarsa (*expiration*), tiket yang sama dapat digunakan berulang kali untuk memasukkan banyak orang. Sung dkk. (2015) menyarankan penggunaan kedaluwarsa pada kode untuk membatalkan validitasnya setelah jangka waktu tertentu guna mematahkan serangan ini.

c) Eksfiltrasi Data dan Pencurian Kunci (*Data & Key Exfiltration*): Serangan ini menargetkan penyimpanan lokal (*local storage*) pada perangkat pengguna. Sung dkk. (2015) menjelaskan bahwa data sensitif yang disimpan di perangkat rentan diakses oleh perangkat lunak berbahaya (*malware*). Dalam konteks *e-ticket*, jika penyerang berhasil mencuri kunci rahasia pembangkit token (*seed key*) atau data pribadi pengguna (*PII*) yang tersimpan, mereka dapat melakukan pengambilalihan akun atau merekonstruksi tiket valid secara ilegal. Ancaman ini menuntut penerapan prinsip *Data Minimization* dan penyimpanan kunci yang aman.

d) Rekayasa Balik (*Reverse Engineering*): Serangan ini menargetkan logika aplikasi pemindai atau aplikasi pengguna. Penyerang mencoba membongkar kode sumber aplikasi untuk menemukan kunci enkripsi statis (*hardcoded keys*) atau algoritma validasi yang digunakan. Jika penyerang berhasil mendapatkan kunci utama (*Master Secret*) dari aplikasi pemindai, mereka dapat memalsukan tiket valid secara massal tanpa terdeteksi oleh sistem *offline*. Risiko ini menegaskan pentingnya perlindungan fisik dan logik pada perangkat pemindai.

II.4 Landasan Teori Kriptografi untuk Solusi

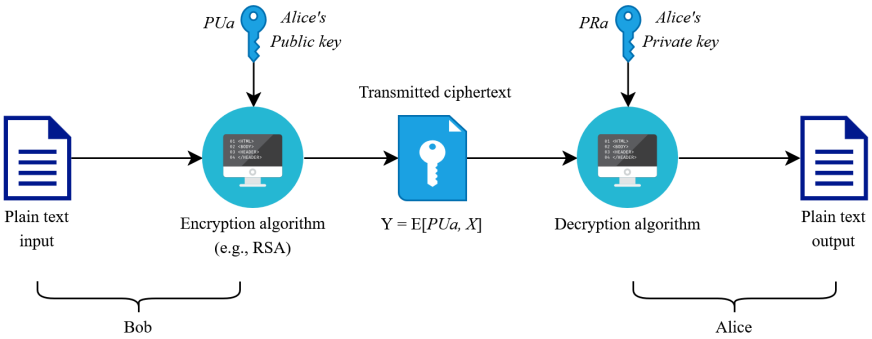
Solusi keamanan yang diusulkan dalam penelitian ini, yaitu *Dynamic Secure QR Code*, dibangun di atas fondasi algoritma kriptografi modern. Subbab ini akan menguraikan konsep teoretis dari teknologi kriptografi yang digunakan, meliputi kriptografi asimetris sebagai kerangka kerja utama, tanda tangan digital untuk menjamin aspek nirsangkal, serta algoritma *Time-based One-Time Password* (TOTP) sebagai mekanisme pembaruan kode secara dinamis.

II.4.1 Kriptografi Asimetris (*Public-Key Cryptography*)

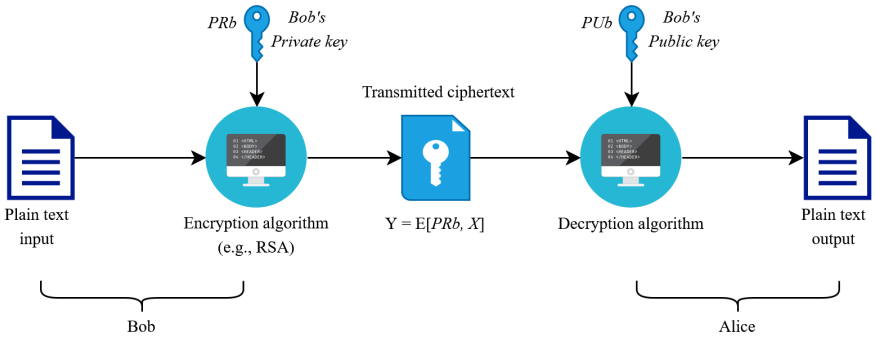
Kriptografi asimetris, atau sering disebut kriptografi kunci publik, merupakan konsep fundamental dalam keamanan informasi modern yang diperkenalkan untuk mengatasi kelemahan distribusi kunci pada kriptografi simetris. Stallings (2022) menjelaskan bahwa skema ini menggunakan dua kunci berbeda yang saling berkaitan secara matematis, yaitu kunci publik dan kunci privat.

Stallings (2022) menjelaskan, skema enkripsi kunci publik terdiri dari enam komponen utama yang saling berinteraksi, sebagaimana diilustrasikan pada Gambar II.2. Komponen-komponen tersebut adalah:

a) *Plaintext*: Ini adalah pesan atau data asli yang dapat dibaca (*readable*) yang dimasukkan ke dalam algoritma sebagai input.
b) Algoritma Enkripsi: Algoritma yang melakukan berbagai transformasi matematis terhadap *plaintext* untuk mengubahnya menjadi bentuk yang tidak dapat dibaca.
c) Kunci Publik dan Privat: Sepasang kunci yang telah dipilih sedemikian rupa sehingga jika salah satu digunakan untuk enkripsi, maka kunci pasangannya digunakan untuk dekripsi. Transformasi pasti yang dilakukan oleh algoritma bergantung pada kunci publik atau privat yang diberikan sebagai input.



(a) Enkripsi Kunci Publik (Kerahasiaan)



(b) Enkripsi Kunci Privat (Autentikasi)

Gambar II.2 Skema Enkripsi Kunci Publik (Stallings 2022)

d) *Ciphertext*: Pesan terenkripsi atau teracak yang dihasilkan sebagai output. *Ciphertext* bergantung pada *plaintext* dan kunci yang digunakan. Untuk pesan yang sama, dua kunci yang berbeda akan menghasilkan dua *ciphertext* yang berbeda.

e) Algoritma Dekripsi: Algoritma yang menerima *ciphertext* dan kunci pasangan yang cocok (kunci privat jika dienkripsi dengan publik, atau sebaliknya), lalu menghasilkan kembali *plaintext* asli.

Mekanisme kerja sistem ini didasarkan pada fungsi satu arah (*one-way function*). Meskipun secara teoretis dapat digunakan untuk kerahasiaan (*confidentiality*) melalui enkripsi pesan seperti yang ditunjukkan Gambar II.2a, dalam penelitian ini fungsi utama kriptografi asimetris difokuskan pada aspek autentikasi dan integritas data (Gambar II.2b). Kunci privat digunakan oleh pengirim (server) untuk menandatangani data, sedangkan kunci publik digunakan oleh penerima (pemindai) untuk memverifikasi keasliannya tanpa perlu mengetahui kunci privat tersebut.

Pada pengerjaan tugas akhir ini, secara spesifik akan memanfaatkan algoritma *Ellip-*

tic Curve Cryptography (ECC). Berbeda dengan algoritma RSA yang mendasarkan keamanannya pada faktorisasi bilangan prima besar, ECC mendasarkan keamanannya pada masalah logaritma diskrit kurva eliptik (*Elliptic Curve Discrete Logarithm Problem*). Keunggulan utama ECC adalah efisiensi sumber daya yang dijelaskan Bafandehkar dkk. (2013) dalam studi perbandingannya, menunjukkan bahwa ECC mampu memberikan tingkat keamanan yang setara dengan RSA namun dengan ukuran kunci yang jauh lebih kecil. Karakteristik ini menjadikan ECC sangat ideal untuk diimplementasikan pada perangkat dengan sumber daya komputasi terbatas seperti ponsel pintar dalam sistem *e-ticket*, yang efisiensi pemrosesan dan ukuran data (*payload*) menjadi prioritas utama.

II.4.2 Tanda Tangan Digital (*Digital Signature*)

Tanda tangan digital adalah mekanisme kriptografi yang berfungsi sebagai analog digital dari tanda tangan tulisan tangan, namun dengan tingkat keamanan yang jauh lebih tinggi karena melekat secara matematis pada dokumen yang ditandatangani. Menurut Stallings (2022), tanda tangan digital memberikan tiga jaminan keamanan utama: autentikasi sumber (memastikan pengirim adalah pihak yang sah), integritas data (memastikan data tidak diubah sejak ditandatangani), dan nirsangkal (*non-repudiation*) (pengirim tidak dapat menyangkal telah mengirim pesan tersebut).

Proses pembuatan tanda tangan digital melibatkan penggunaan fungsi *hash* dan kunci privat pengirim. Data atau pesan (*message*) terlebih dahulu diproses melalui fungsi *hash* untuk menghasilkan nilai ringkasan (*digest*) yang unik. Nilai *hash* ini kemudian dienkripsi menggunakan kunci privat pengirim untuk membentuk tanda tangan digital. Pada sisi penerima (verifikator), proses validasi dilakukan dengan mendekripsi tanda tangan menggunakan kunci publik pengirim untuk mendapatkan nilai *hash* asli, dan membandingkannya dengan nilai *hash* yang dihitung ulang dari data yang diterima. Jika kedua nilai tersebut identik, maka integritas dan keaslian data terjamin. Dalam penelitian ini, algoritma yang digunakan adalah *Elliptic Curve Digital Signature Algorithm* (ECDSA), yang merupakan varian dari DSA (*Digital Signature Algorithm*) yang beroperasi pada grup kurva eliptik.

II.4.3 HMAC dan Derivasi Kunci (*Key Derivation*)

Hash-based Message Authentication Code (HMAC) adalah konstruksi spesifik untuk menghitung *message authentication code* (MAC) yang melibatkan fungsi *hash* kriptografis yang dikombinasikan dengan kunci rahasia. Sesuai standar RFC 2104, HMAC menyediakan cara untuk memverifikasi integritas informasi sekaligus au-

tentikasi asal pengirim.

Selain untuk autentikasi, properti pseudorandom dari HMAC membuatnya ideal digunakan sebagai Fungsi Derivasi Kunci atau *Key Derivation Function* (KDF). NIST SP 800-108 merekomendasikan penggunaan HMAC dalam mode *Counter* atau *Feedback* untuk menurunkan kunci-kunci kriptografi baru dari sebuah kunci induk (*Master Key*). Secara matematis, kunci turunan ($K_{derived}$) dapat dihasilkan dengan rumus:

$$K_{derived} = HMAC(K_{master}, Context) \tag{II.1}$$

Dalam arsitektur sistem yang terdistribusi, mekanisme ini memungkinkan entitas (seperti alat pemindai) untuk merekonstruksi kunci spesifik milik pengguna hanya dengan mengetahui ID pengguna ($Context$) dan Kunci Induk, tanpa perlu menyimpan basis data kunci yang besar. Konsep ini menjadi fondasi bagi mekanisme validasi *stateless* dan *offline*.

II.4.4 *Time-based One-Time Password* (TOTP)

Untuk mencapai karakteristik dinamis pada sistem *e-ticket*, penelitian ini mengadopsi algoritma *Time-based One-Time Password* (TOTP). TOTP merupakan pengembangan dari algoritma *HMAC-based One-Time Password* (HOTP) yang didefinisikan dalam standar IETF RFC 4226. HOTP membangkitkan kata sandi sekali pakai berdasarkan penghitung kejadian (*event counter*) yang disinkronisasi antara klien dan server. Rumus dasar HOTP didefinisikan sebagai berikut:

$$HOTP(K, C) = Truncate(HMAC\text{-}SHA\text{-}1(K, C)) \tag{II.2}$$

Keterangan:

- K adalah kunci rahasia bersama (*shared secret key*).
- C adalah nilai pencacah (*counter*).
- $HMAC\text{-}SHA\text{-}1$ adalah fungsi *keyed-hash message authentication code*.

Namun, HOTP memiliki kelemahan potensial berupa desinkronisasi jika tombol pembangkit ditekan berulang kali tanpa validasi ke server. Untuk mengatasi hal ini, diperkenalkan TOTP melalui standar RFC 6238. TOTP menggantikan nilai pencacah (C) dengan nilai waktu terkini. Algoritma ini menggunakan interval waktu (*time step*) sebagai faktor pengubah, sehingga kode yang dihasilkan akan valid hanya dalam jendela waktu tertentu (misalnya 30 detik).

Perhitungan nilai langkah waktu (T) dalam TOTP dirumuskan sebagai berikut:

$$T = \lfloor \frac{CurrentTime - T0}{X} \rfloor \tag{II.3}$$

Keterangan:

- $CurrentTime$ adalah waktu saat ini dalam detik (biasanya format *Unix epoch*).
- $T0$ adalah waktu awal penghitungan (biasanya 0).
- X adalah durasi langkah waktu (*time step*), yang secara *default* adalah 30 detik.

Dengan demikian, nilai TOTP dibangkitkan dengan memasukkan nilai T ke dalam fungsi HOTP:

$$TOTP = HOTP(K, T) \tag{II.4}$$

Penggunaan TOTP menjamin bahwa kode QR akan selalu berubah secara periodik mengikuti waktu server. Hal ini memitigasi risiko serangan penggandaan tiket (*cloning attack*) dan serangan putar ulang (*replay attack*) akibat penggunaan tiket hasil tangkapan layar yang telah kedaluwarsa.

II.5 Mekanisme Sinkronisasi Data dan Penyimpanan Lokal

Untuk memitigasi risiko kegagalan jaringan dan meningkatkan kinerja sistem pada lingkungan dengan konektivitas terbatas, penelitian ini menerapkan mekanisme pengelolaan data hibrida.

II.5.1 Manajemen *Cache* Lokal

Penyimpanan sementara atau *caching* adalah teknik fundamental untuk efisiensi data. Tang dkk. (2006) menyatakan bahwa *caching* data secara lokal pada node jaringan dapat secara signifikan meningkatkan efisiensi akses informasi dengan mengurangi latensi akses dan penggunaan *bandwidth* jaringan. Dalam konteks validasi tiket, *cache* lokal pada alat pemindai berfungsi untuk menyimpan riwayat transaksi dan status penggunaan tiket (misalnya: *ticket_id* X sudah masuk pukul Y). Hal ini memungkinkan proses pengecekan duplikasi (*double-spending check*) tetap berjalan secara *real-time* dan konsisten meskipun perangkat sedang tidak terhubung ke

internet.

II.5.2 Sinkronisasi Asinkron (*Batching*)

Selain penyimpanan lokal, efisiensi pengiriman data ke server pusat juga menjadi perhatian utama. Ramachandra dkk. (2015) menjelaskan bahwa pengiriman permintaan data secara asinkron dan terkelompok (*batched*) dapat meningkatkan kinerja aplikasi secara signifikan dibandingkan pengiriman sinkron satu per satu. Teknik ini memungkinkan aplikasi untuk menumpuk log transaksi (seperti status *check-in*) di sisi klien dan mengirimkannya ke server secara kolektif saat koneksi tersedia atau dalam interval waktu tertentu. Pendekatan ini mengurangi penundaan (*delay*) akibat putaran jaringan (*network round-trips*) yang berulang dan memastikan antrean pengunjung tidak terhambat oleh proses sinkronisasi data.

II.6 Penelitian Terkait

Pengembangan sistem keamanan berbasis kode QR telah menjadi subjek penelitian yang aktif dalam beberapa tahun terakhir seiring dengan meningkatnya ancaman digital. Subbab ini meninjau secara mendalam beberapa penelitian terdahulu yang relevan untuk memetakan posisi dan kontribusi penelitian ini. Tinjauan dilakukan terhadap tiga perspektif utama, yaitu: (1) mekanisme anti-pemalsuan pada media fisik, (2) analisis kerentanan pada autentikasi seluler, dan (3) studi implementasi kode QR dinamis.

II.6.1 Sistem kode QR Anti-Pemalsuan Berbasis *Watermarking* dan CNN (Alsuhibany 2025)

Dalam studi ini, Alsuhibany (2025) mengembangkan sistem untuk memitigasi ancaman substitusi kode batang (*barcode substitution fraud*) dan serangan pencetakan ulang (*reprinting attack*) yang sering terjadi pada label produk dan dokumen fisik. Alsuhibany (2025) mengidentifikasi bahwa kode QR standar tidak memiliki fitur keamanan inheren, sehingga pelaku kejahatan dapat dengan mudah menyalin atau mengganti kode asli dengan kode palsu untuk memanipulasi informasi produk. Hal ini tidak hanya menyebabkan kerugian finansial, tetapi juga merusak kepercayaan konsumen sehingga memerlukan pengawasan manual yang lebih ketat.

Untuk mengatasi masalah tersebut, penelitian ini mengusulkan pendekatan keamanan dua lapis. Lapisan pertama adalah mekanisme *tamper-proof generation* menggunakan teknik *digital watermarking* pada domain spasial. Teknik ini menyisipk-

an pola keamanan unik (yang berbeda untuk setiap pasar) ke dalam citra kode QR menggunakan metode modifikasi *Least Significant Bit* (LSB). Penulis mengklaim bahwa metode ini dipilih karena kesederhanaannya dan ketahanannya terhadap distorsi umum seperti pencetakan dan pemindaian ulang. Lapisan kedua adalah mekanisme verifikasi berbasis kecerdasan buatan (*Artificial Intelligence*) menggunakan *Convolutional Neural Network* (CNN). Model tersebut dilatih untuk mendeteksi perbedaan mikroskopis atau degradasi kualitas (*noise*) yang membedakan antara kode QR asli dan hasil cetak ulang (*reprinted*).

Meskipun metode ini terbukti efektif dalam mendeteksi pemalsuan pada media fisik, pendekatannya memiliki keterbatasan jika diterapkan pada tiket digital berbasis layar ponsel yang memerlukan proses verifikasi cepat dan ringan. Dalam ekosistem *e-ticket*, ancaman utama adalah duplikasi melalui tangkapan layar (*screenshot*) yang menghasilkan salinan digital identik secara bit-per-bit tanpa degradasi fisik, sehingga sulit dideteksi oleh model CNN. Oleh karena itu, penelitian Tugas Akhir ini akan melengkapi pendekatan analisis citra statis tersebut dengan mekanisme kriptografi dinamis (TOTP) yang jauh lebih ringan secara komputasi dan memungkinkan validasi dilakukan secara mandiri (*offline*) pada perangkat pemindai.

II.6.2 Analisis Kerentanan Autentikasi Seluler Berbasis kode QR (Sung dkk. 2015)

Penelitian yang dilakukan oleh Sung dkk. (2015) menyajikan analisis keamanan komprehensif terhadap sistem autentikasi yang menggunakan kode QR pada perangkat seluler. Berbeda dengan pandangan umum yang menganggap kode QR aman, penelitian ini mengungkap berbagai vektor serangan kritis, khususnya yang terjadi pada sisi klien (*client-side*).

Sung dkk. (2015) mengklasifikasikan kerentanan tersebut ke dalam beberapa kategori utama. Pertama, kerentanan penggandaan (*cloning*), adalah ketika kode QR mudah disalin melalui fitur tangkapan layar (*screen capture*) karena sistem tidak dapat membedakan citra asli di aplikasi dengan citra salinan. Kedua, serangan putar ulang (*replay attack*) yang terjadi ketika kode valid digunakan kembali di luar waktu yang diizinkan. Ketiga, eksfiltrasi data (*stored data exfiltration*), yaitu risiko pencurian data kredensial yang tersimpan di memori lokal perangkat oleh aplikasi berbahaya (*malware*) jika tidak dilindungi dengan memadai.

Sebagai usulan mitigasi, Sung dkk. (2015) merekomendasikan kerangka kerja implementasi aman yang mencakup penerapan mekanisme kedaluwarsa (*expiration*)

untuk mencegah serangan putar ulang dan enkripsi penyimpanan. Mengadaptasi temuan tersebut, penelitian Tugas Akhir ini menerapkan algoritma TOTP untuk manajemen kedaluwarsa otomatis. Namun, berbeda dengan pendekatan enkripsi data tiket yang direkomendasikan, penelitian ini memilih pendekatan *Data Minimization* dan *Privacy by Design*. Dengan tidak menyertakan data pribadi sensitif dalam *payload* kode QR, risiko eksfiltrasi data dapat dimitigasi tanpa membebani kinerja pemindaian dengan proses dekripsi yang berat.

II.6.3 Studi Komparasi kode QR Statis dan Dinamis (Yanuarafi 2023)

Dalam konteks implementasi sistem autentikasi kehadiran, Yanuarafi (2023) melakukan studi komparatif antara penggunaan kode QR statis dan dinamis pada sistem presensi pegawai di lingkungan universitas. Penelitian ini dilatarbelakangi oleh maraknya kecurangan presensi yang terjadi akibat kelemahan sistem statis, yang terjadi akibat kode identitas yang bersifat tetap mudah disalin dan dibagikan kepada rekan kerja untuk melakukan presensi palsu ("titip absen").

Hasil penelitian menunjukkan bahwa kode QR dinamis memiliki keunggulan signifikan dalam aspek keamanan dibandingkan varian statis. Dengan mekanisme perubahan kode secara berkala, celah keamanan berupa penggunaan ulang kode (*reuse*) atau penggandaan kode statis dapat diminimalisasi secara efektif. Yanuarafi (2023) menyimpulkan bahwa meskipun implementasi sistem dinamis membutuhkan sumber daya komputasi yang lebih besar, tingkat akurasi dan keamanan data yang dihasilkan jauh lebih tinggi, menjadikannya standar yang direkomendasikan.

Meskipun penelitian ini berhasil membuktikan keunggulan konsep dinamis, fokus utamanya terletak pada fungsionalitas aplikasi presensi secara *online*. Penelitian tersebut belum membahas mekanisme perlindungan integritas data secara kriptografis untuk skenario konektivitas terbatas. Celah inilah yang akan dilengkapi oleh penelitian Tugas Akhir ini melalui arsitektur *Dynamic Secure QR Code* yang tidak hanya bersifat dinamis, tetapi juga dilengkapi Tanda Tangan Digital dan mekanisme validasi *stateless* agar tetap andal digunakan dalam kondisi *offline*.

II.6.4 Posisi Penelitian dan Kontribusi

Berdasarkan tinjauan literatur di atas, dapat dipetakan bahwa penelitian-penelitian terdahulu umumnya berfokus pada salah satu aspek keamanan secara terpisah. Belum banyak ditemukan sistem yang mengintegrasikan mekanisme pertahanan secara holistik untuk menjawab tiga kebutuhan utama keamanan tiket, yaitu: (1) Aspek di-

namis untuk mencegah serangan penggandaan, (2) aspek privasi untuk melindungi data pengguna dari eksfiltrasi, dan (3) aspek integritas untuk menjamin keaslian penerbit tiket.

Penelitian ini bertujuan mengisi celah penelitian (*research gap*) tersebut dengan mengusulkan arsitektur *Dynamic Secure QR Code*. Kontribusi utama penelitian ini adalah penggabungan algoritma TOTP, Tanda Tangan Digital (ECDSA), dan mekanisme *Key Derivation* yang memungkinkan validasi tiket dilakukan secara aman, cepat, dan *offline* tanpa mengorbankan privasi data pengguna. Perbandingan posisi penelitian ini dengan penelitian terkait dapat dilihat pada Tabel II.2.

Tabel II.2 Perbandingan Fitur Keamanan Penelitian Terkait dengan Penelitian yang Diusulkan

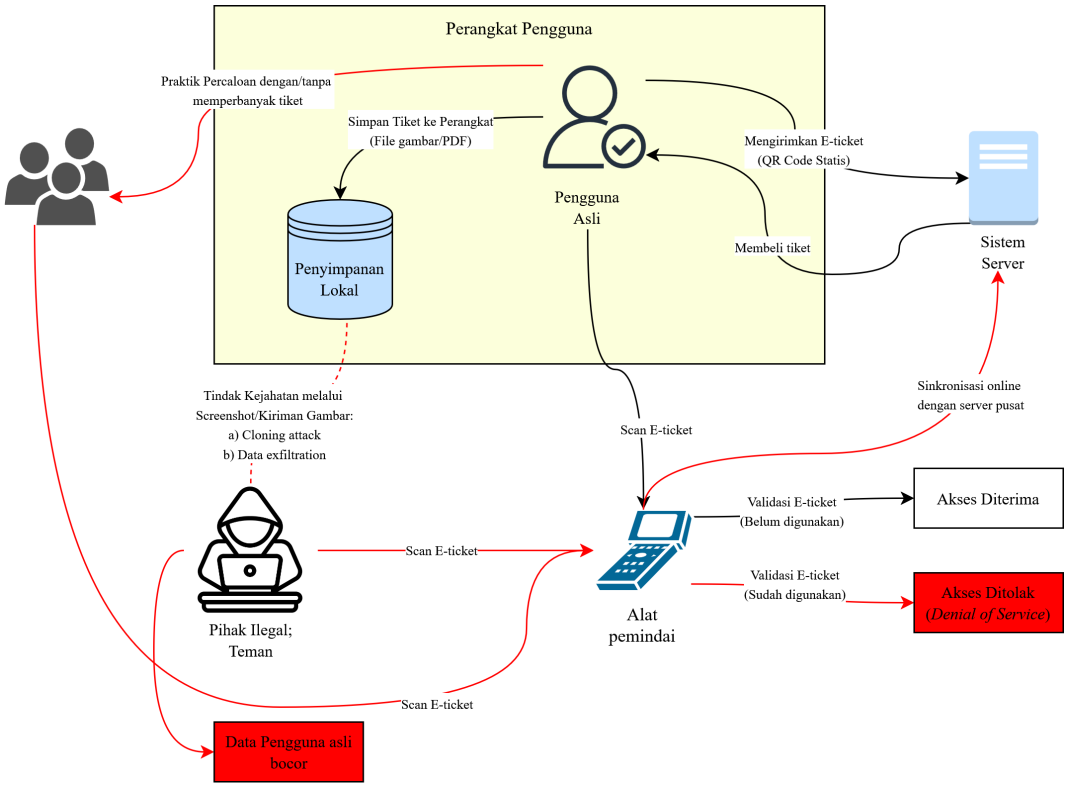
Peneliti	**Fokus Penelitian**	**Dinamis**	**Privasi**	**Integritas**
Sung dkk. (2015)	Analisis kerentanan autentikasi *mobile*	Saran	Saran	-
Alsuhibany (2025)	*Watermarking* digital pada media cetak	Tidak	Tidak	Ya
Yanuarafi (2023)	Perbandingan presensi statis vs dinamis	Ya	Tidak	-
Penelitian Ini	**Sistem *E-Ticket* (TOTP + Data Minimization + TTD)**	**Ya**	**Ya**	**Ya**

BAB III

ANALISIS MASALAH

III.1 Analisis Kondisi Saat Ini

Berdasarkan tinjauan terhadap sistem pertiketan elektronik konvensional yang umum digunakan saat ini (seperti pada studi kasus konser musik dan pertandingan olahraga), model proses bisnis yang berjalan masih mengandalkan arsitektur kode QR statis. Model konseptual dari sistem yang berjalan, beserta titik-titik kerentanan yang teridentifikasi dalam alur distribusi dan validasi tiket, digambarkan pada Gambar III.1.



Gambar III.1 Model Konseptual dan Titik Kerentanan Sistem *E-Ticket* Konvensional

Sebagaimana diilustrasikan pada Gambar III.1, proses dimulai ketika pengguna asli membeli tiket dari sistem server. Tiket yang dibangkitkan kemudian dikirim dan disimpan ke dalam penyimpanan lokal perangkat pengguna dalam format berkas statis (seperti gambar atau PDF). Sifat data yang statis dan tersimpan secara lokal ini menciptakan celah keamanan yang digambarkan melalui empat vektor ancaman utama pada diagram:

1. Distribusi Tiket Tidak Terkendali (Praktik Percaloan): Seperti terlihat pada alur panah merah bagian atas diagram, ketiadaan mekanisme validasi berbasis waktu (*time-based validation*) memungkinkan pengguna asli untuk mendistribusikan satu tiket kepada banyak pihak lain hanya dengan menyalin citra kode QR. Karena kode tersebut berlaku tanpa batas waktu hingga dipindai (statis), tiket dapat digandakan dan dijual kembali dengan mudah tanpa terikat pada sesi aplikasi pengguna yang sah. Hal ini menyuburkan praktik percaloan, yaitu ketika tiket dijual dengan harga yang melambung tinggi tanpa kendali penyelenggara resmi sehingga merusak ekosistem penjualan tiket yang sehat.
2. Ancaman Penggandaan (*Cloning Attack*) dan Penolakan Layanan: Celah pada penyimpanan lokal memungkinkan pihak ilegal mengambil alih tiket melalui tangkapan layar (*screenshot*). Hal ini menciptakan kondisi "balapan" ke para pemilik tiket yang identik, untuk diverifikasikan pada alat pemindai. Sebagaimana ditunjukkan pada alur validasi diagram, jika pihak ilegal berhasil memindai tiket lebih awal, maka alat pemindai akan mencatat tiket sebagai "Sudah Digunakan". Akibatnya, pengguna asli yang datang belakangan akan mengalami penolakan akses (*Denial of Service*), meskipun memiliki tiket yang sah secara pembelian.
3. Kebocoran Data Pribadi (*Data Exfiltration*): Penyimpanan tiket statis tanpa perlindungan memadai pada penyimpanan lokal membuka peluang terjadinya eksfiltrasi data. Informasi sensitif pengguna yang melekat pada tiket (seperti nama, nomor ponsel, atau identitas penting lainnya) dapat dengan mudah terbaca apabila dokumen *e-ticket* tersebut jatuh ke tangan pihak tidak bertanggung jawab, sebagaimana digambarkan pada blok "Data Pengguna Asli Bocor".
4. Ketergantungan Konektivitas (*Single Point of Failure*): Sebagaimana ditunjukkan oleh garis alur "Sinkronisasi online dengan server pusat", mekanisme validasi saat ini mewajibkan alat pemindai untuk terus terhubung ke server guna memverifikasi status tiket. Hal ini menciptakan risiko *Single Point of Failure* (SPOF). Apabila terjadi gangguan jaringan di lokasi acara atau kelebihan beban (*server overload*), proses validasi akan terhenti total. Kondisi ini

tidak hanya menghambat antrean masuk (*bottleneck*), tetapi juga mengancam ketersediaan layanan (*Availability*) di titik krusial acara.

Kondisi ini menegaskan bahwa sistem saat ini belum memenuhi prinsip keamanan CIA Triad (*Confidentiality, Integrity, Availability*) yang memadai untuk menangani transaksi tiket bernilai tinggi.

III.2 Analisis Kebutuhan

Tahap analisis kebutuhan bertujuan untuk mendefinisikan spesifikasi sistem yang harus dipenuhi guna mengatasi permasalahan yang telah diidentifikasi pada model sistem saat ini. Analisis ini dibagi menjadi identifikasi masalah pengguna, kebutuhan fungsional, dan kebutuhan non-fungsional.

III.2.1 Identifikasi Masalah Pengguna

Berdasarkan analisis kondisi saat ini, terdapat beberapa permasalahan kritis yang dihadapi oleh pemangku kepentingan utama, yaitu penyelenggara acara (*event organizer*) dan pengguna (pemegang tiket yang sah). Masalah-masalah tersebut diuraikan sebagai berikut:

1. Distribusi Tiket Tidak Terkendali: Pada sistem saat ini, tiket yang telah dibeli dapat dipindahtangankan atau diperjualbelikan kembali dengan sangat mudah melalui pengiriman citra digital (tangkapan layar). Akar masalahnya adalah sifat statis dari visualisasi kode QR, yang informasi validitas tiketnya melekat permanen pada citra tanpa batasan waktu tayang. Akibatnya, sistem tidak dapat membedakan antara pemegang tiket asli yang mengakses melalui aplikasi resmi dengan pihak lain yang hanya bermodalkan tangkapan layar, sehingga menyuburkan praktik percaloan dan merugikan konsumen akibat harga jual yang dimanipulasi.
2. Penolakan Layanan akibat Penggandaan (*Denial of Service*): Pemegang tiket yang sah berisiko gagal memasuki area acara jika tiket mereka telah digandakan (*cloning*) dan digunakan lebih dulu oleh pihak lain. Dalam sistem QR statis, alat pemindai tidak dapat membedakan mana pemilik asli dan mana pembawa salinan. Kondisi ini menciptakan "kompetisi" (*race condition*) di pintu masuk; siapa yang memindai lebih dulu akan diterima, sedangkan yang datang belakangan—meskipun pemilik sah—akan tertolak sistem karena status tiket dianggap sudah terpakai.
3. Masalah Privasi Data: Pengguna menghadapi risiko keamanan data karena informasi pribadi (seperti NIK, Nama, dan Detail Pesanan) yang melekat pada

tiket digital tersimpan dalam format teks asli (*plaintext*). Tanpa mekanisme penanganan yang tepat seperti enkripsi atau minimalisasi data (*data minimization*), informasi ini rentan dicuri (*data exfiltration*) dan disalahgunakan.

4. Ketergantungan Koneksi dan Titik Kegagalan Tunggal: Proses pemindaian tiket konvensional umumnya bergantung penuh pada koneksi internet ke server pusat untuk memverifikasi setiap kali pemindaian (*online verification*). Ketergantungan ini menciptakan risiko Titik Kegagalan Tunggal (*Single Point of Failure*). Risiko ini muncul apabila terputusnya koneksi server, baik karena gangguan infrastruktur ataupun akibat saturasi jaringan seluler (banjir trafik), yang menyebabkan seluruh proses pemindaian di gerbang terhenti total sehingga terjadinya kekacauan antrean dan operasional.

III.2.2 Kebutuhan Fungsional

Kebutuhan fungsional mendefinisikan layanan atau fitur spesifik yang harus disediakan oleh sistem untuk menjawab masalah pengguna di atas. Rincian kebutuhan fungsional sistem *Dynamic Secure QR Code* dijabarkan pada Tabel III.1.

Tabel III.1 Daftar Kebutuhan Fungsional Sistem

Kode	**Kebutuhan Fungsional**	**Deskripsi**
FR-01	Penerbitan *E-ticket*	Sistem (Server) dapat menerbitkan tiket elektronik baru yang berisi atribut tiket (ID dan metadata), kunci rahasia spesifik pengguna (*user secret key*), dan tanda tangan digital, lalu mendistribusikannya secara aman ke perangkat pengguna.
FR-02	Pembangkitan kode QR Dinamis	Sistem (Aplikasi Pengguna) dapat memvisualisasikan tiket dalam bentuk kode QR dinamis yang muatan datanya diperbarui otomatis setiap interval waktu tertentu (misalnya 30 detik) berdasarkan token dinamis TOTP.
FR-03	Minimalisasi Data & Privasi	Sistem menerapkan prinsip *Data Minimization* dengan membatasi muatan data kode QR hanya pada atribut teknis non-sensitif (ID Tiket dan Metadata), sehingga informasi pribadi pengguna tidak terekspos dalam *payload* kode QR.

Bersambung ke halaman berikutnya

Tabel III.1 Daftar Kebutuhan Fungsional Sistem (lanjutan)

Kode	Kebutuhan Fungsional	Deskripsi
FR-04	Integritas Data Tiket	Sistem menyertakan mekanisme penandatanganan digital (*Digital Signature*) pada data tiket untuk menjamin keaslian penerbit dan memastikan informasi tidak dimodifikasi.
FR-05	Verifikasi Lokal *Stateless*	Aplikasi pemindai (*Scanner*) dapat memverifikasi tanda tangan digital dan validitas token TOTP secara mandiri (*offline*) menggunakan mekanisme derivasi kunci, tanpa membutuhkan koneksi internet ke server pusat.
FR-06	Validasi Token Waktu	Aplikasi pemindai dapat memverifikasi kebenaran token dinamis yang dibawa pengguna dengan menyertakan mekanisme toleransi sinkronisasi waktu, guna mengantisipasi perbedaan jam internal (*clock drift*).
FR-07	Manajemen *Cache* Lokal	Aplikasi pemindai memiliki penyimpanan sementara (*local cache*) untuk mencatat ID tiket yang baru saja dipindai guna mencegah serangan penggandaan instan (*replay/cloning attack*).
FR-08	Sinkronisasi Asinkron (*Batching*)	Sistem mendukung pengiriman data log kehadiran secara berkala (*batching*) dari pemindai ke server pusat di latar belakang untuk efisiensi lalu lintas jaringan.

III.2.3 Kebutuhan Non-fungsional

Kebutuhan non-fungsional mendefinisikan atribut kualitas, batasan operasional, dan standar kinerja yang harus dipenuhi sistem. Rincian kebutuhan non-fungsional dijabarkan pada Tabel III.2.

Tabel III.2 Daftar Kebutuhan Non-fungsional Sistem

Kode	**Parameter**	**Deskripsi**
NFR-01	Keamanan (*Security*)	Sistem harus menerapkan Tanda Tangan Digital untuk integritas dan prinsip *Privacy by Design* untuk kerahasiaan data pribadi, serta memastikan ketahanan terhadap upaya pemalsuan tiket.
NFR-02	Kinerja (*Performance*)	Proses pembangkitan kode QR di sisi pengguna dan proses verifikasi kriptografi di sisi pemindai harus dapat diselesaikan dalam waktu kurang dari 2 detik (latensi rendah).
NFR-03	Ketersediaan (*Availability*)	Fitur validasi tiket utama harus memiliki tingkat ketersediaan tinggi dan tetap berfungsi penuh dalam mode *offline* (tanpa koneksi internet).
NFR-04	Kompatibilitas (*Compatibility*)	Sistem harus kompatibel dengan perangkat seluler lintas platform (Android dan iOS) serta tidak mensyaratkan ketersediaan perangkat keras khusus selain kamera standar.

III.3 Analisis Pemilihan Solusi

Berdasarkan identifikasi masalah yang kompleks, yaitu kebutuhan akan keamanan tinggi (anti-pemalsuan) yang berbenturan dengan kebutuhan operasional (ketersediaan sistem saat jaringan padat), diperlukan analisis mendalam untuk menentukan pendekatan solusi terbaik. Bagian ini akan menguraikan berbagai alternatif solusi yang mungkin diterapkan, mulai dari pendekatan visual sederhana hingga pendekatan berbasis perangkat keras, kemudian mengevaluasinya berdasarkan metrik yang terukur.

III.3.1 Alternatif Solusi

Terdapat empat kandidat solusi (alternatif) yang diidentifikasi dapat menjawab sebagian atau seluruh permasalahan sistem pertiketan saat ini. Evaluasi setiap alternatif adalah sebagai berikut:

1. Alt-01: Validasi Tambahan Untuk *E-ticket* secara Visual (*Watermarking*): Alternatif solusi pertama menggunakan pendekatan visual dengan memberi *wa-*

termarking pada kode QR. Pendekatan ini menyelesaikan masalah penggandaan dengan menambahkan elemen visual pada desain tiket yang unik, membedakannya dari visual kode QR biasa sehingga petugas dapat mengenali keasliannya secara manual. Elemen visual yang ditambahkan dapat berupa latar belakang khusus, logo, atau gambar animasi/GIF (*Graphic Interchange Format*) yang sulit ditiru. Elemen visual yang diterapkan pada kode QR, akan dinamis berdasarkan rentang waktu tertentu (misalnya berganti setiap jam) sehingga menambah tingkat kesulitan dalam meniru desain tiket. Dengan demikian, meskipun kode QR dapat disalin, elemen visual tambahan akan menjadi indikator penentu keaslian tiket sehingga mencegah *cloning* dan pemalsuan tiket. Keunggulan yang paling menonjol dari pendekatan ini adalah biaya implementasi yang relatif rendah dan tidak memerlukan teknologi canggih. Namun, kelemahan utamanya adalah efektivitasnya, yang tidak dapat mengatasi sepenuhnya ancaman penggandaan melalui rekaman layar (*screen recording*). Selain itu, alternatif solusi ini rentan terhadap kesalahan manusia (*human error*) karena *watermark* harus diperiksa secara manual oleh petugas. Dalam proses verifikasi visual di gerbang masuk, risiko *human error* dapat mengakibatkan tiket palsu lolos verifikasi jika petugas tidak teliti. Oleh karena itu, meskipun pendekatan ini menambah lapisan keamanan, namun tidak cukup kuat untuk menghadapi ancaman modern yang semakin canggih.

2. Alt-02: Validasi Tiket Berbasis Perangkat Keras (NFC/RFID): Alternatif kedua menawarkan perubahan fundamental dari validasi berbasis optik (kamera) menjadi validasi berbasis frekuensi radio menggunakan teknologi *Near Field Communication* (NFC). Dalam skema ini, data tiket tidak lagi ditampilkan di layar, melainkan disimpan secara aman di dalam elemen aman (*Secure Element*) atau emulasi kartu pada perangkat seluler pengguna. Mekanisme validasi dilakukan dengan cara menempelkan perangkat pengguna ke gerbang masuk (*tap-to-enter*), yang memungkinkan pertukaran kunci kriptografi secara instan antar-perangkat keras. Keunggulan utama pendekatan ini adalah tingkat keamanan yang sangat tinggi, karena tiket terikat pada perangkat keras (*hardware-bound*) sehingga hampir mustahil untuk dikloning atau dipindahkan sembarangan. Selain itu, kecepatan proses validasi NFC jauh lebih unggul (kurang dari 0,5 detik) dibandingkan pemindaian visual, yang sangat efektif mengurai antrean. Meskipun demikian, solusi ini memiliki kendala pada aspek kompatibilitas dan biaya. Tidak semua perangkat seluler pengguna, terutama pada segmen *low-end* atau *entry-level* di Indonesia, dilengkapi dengan

fitur NFC. Mewajibkan penggunaan NFC akan membatasi akses layanan bagi sebagian besar pengguna (*exclusionary*). Selain itu, biaya pengadaan infrastruktur gerbang berbasis NFC jauh lebih mahal dibandingkan pemindai optik standar, sehingga kurang efisien dari sisi investasi penyelenggara.

3. Alt-03: Kode QR Dinamis Terpusat (*Online Token*): Pendekatan ketiga mempertahankan penggunaan kode QR, namun mengubah sifat muatan datanya menjadi dinamis dengan kontrol penuh di sisi server pusat. Dalam mekanisme ini, aplikasi pengguna tidak menyimpan data tiket secara statis, melainkan harus melakukan permintaan (*request*) ke server melalui API (*Application Programming Interface*) setiap kali tiket hendak ditampilkan. Server kemudian membangkitkan token QR baru yang hanya berlaku dalam durasi tertentu (misalnya 10 detik) dan mengirimkannya kembali ke aplikasi. Solusi ini sangat efektif menanggulangi masalah tiket statis karena setiap kode QR bersifat sekali pakai atau berdurasi pendek sehingga tangkapan layar lama menjadi tidak berguna. Namun, ketergantungan penuh terhadap koneksi internet menjadi kelemahan kritis dari solusi ini. Dalam skenario acara berskala besar dengan puluhan ribu pengunjung, saturasi jaringan seluler adalah kejadian yang hampir pasti terjadi. Jika perangkat pengguna atau alat pemindai gagal terhubung ke server akibat sinyal buruk, tiket tidak dapat dimuat atau divalidasi. Hal ini menciptakan risiko Titik Kegagalan Tunggal (*Single Point of Failure*) yang dapat menyebabkan kelumpuhan operasional total di pintu masuk, memicu penumpukan massa dan potensi kerusuhan.

4. Alt-04: Kode QR Dinamis Hibrida (Usulan): Alternatif keempat, yang menjadi usulan dalam penelitian ini, menggabungkan keamanan token dinamis dengan keandalan operasional sistem (*offline*). Berbeda dengan Alt-03 yang bergantung pada server, logika pembangkitan token dipindahkan ke sisi perangkat pengguna (*client-side*) menggunakan algoritma *Time-based One-Time Password* (TOTP). Dalam pendekatan ini, muatan (*payload*) kode QR dirancang seminimal mungkin (*Data Minimization*)—hanya berisi atribut teknis non-sensitif—serta dilindungi oleh Tanda Tangan Digital untuk menjamin integritas. Inovasi kunci dari solusi ini terletak pada mekanisme validasi *stateless* menggunakan skema Derivasi Kunci (*Key Derivation*). Melalui skema ini, alat pemindai mampu menurunkan (*derive*) kunci rahasia spesifik pengguna secara mandiri menggunakan *Master Key* internal dan ID tiket yang dipindai. Mekanisme ini memungkinkan validasi keaslian token TOTP dilakukan

secara lokal dan instan tanpa koneksi internet, sekaligus meniadakan risiko keamanan terkait penyimpanan data kunci sensitif pengguna pada perangkat pemindai. Solusi ini menawarkan keseimbangan terbaik antara keamanan (*anti-cloning*), perlindungan privasi, dan ketersediaan layanan (*availability*) di lingkungan dengan konektivitas terbatas.

III.3.2 Analisis Penentuan Solusi

Untuk menentukan solusi yang paling optimal, keempat alternatif di atas dievaluasi menggunakan empat parameter yang diturunkan dari analisis kebutuhan sistem:

1. Keamanan (*Security*): Kemampuan sistem menahan serangan penggandaan dan menjaga integritas data.
2. Ketersediaan (*Availability*): Kemampuan sistem beroperasi dalam kondisi jaringan buruk atau bahkan terputus(*offline*).
3. Kompatibilitas (*Accessibility*): Tingkat dukungan terhadap ragam perangkat pengguna. Solusi yang diusulkan tidak boleh membatasi akses hanya pada pengguna ponsel kelas atas (*flagship*).
4. Efisiensi Operasional: Kecepatan proses validasi di gerbang untuk mencegah penumpukan antrean (*bottleneck*).

Berdasarkan parameter tersebut, berikut adalah analisis perbandingan antar kandidat solusi:

Alt-01 (Visual) dinilai tidak memadai dari sisi Keamanan karena teknik manipulasi visual (rekaman layar) saat ini sudah sangat canggih dan sulit dibedakan oleh mata telanjang petugas (*human error*). Selain itu, ketergantungan pada pemeriksaan manual sangat menurunkan efisiensi operasional.

Alt-02 (NFC) menawarkan skor keamanan dan efisiensi tertinggi karena validasi terjadi secara instan antar-perangkat keras. Namun, solusi ini memiliki kendala pada aspek Kompatibilitas. Mewajibkan fitur NFC akan menghalangi sebagian besar pengguna dengan perangkat menengah ke bawah untuk mengakses tiket mereka, yang bertentangan dengan prinsip inklusivitas layanan publik.

Alt-03 (QR Online) memiliki risiko Ketersediaan yang buruk (*Critical Risk*) karena ketergantungan penuh pada koneksi server saat kerumunan massal. Jika sistem bergantung pada koneksi server untuk mendapatkan tiket, risiko kegagalan sistem total sangat tinggi, yang dapat memicu kerusuhan di lokasi acara.

Alt-04 (Hybrid/Usulan) menawarkan keseimbangan terbaik. Pendekatan ini men-

capai nilai Keamanan yang tinggi (melalui TOTP dan Digital Signature) serta nilai Ketersediaan (*availability*) yang sangat baik karena kemampuan operasi *offline* melalui validasi lokal. Privasi pengguna juga terjaga tanpa memerlukan enkripsi berat pada pemindai.

Rangkuman evaluasi tersebut disajikan dalam Matriks Keputusan pada Tabel III.3.

Tabel III.3 Matriks Keputusan Pemilihan Solusi Sistem *E-Ticket*

Kriteria	**Alt-01** (Visual)	**Alt-02** (NFC)	**Alt-03** (Online)	**Alt-04** (Hybrid)
Keamanan	Buruk	Sangat Baik	Baik	**Baik**
Ketersediaan	Sangat Baik	Sangat Baik	Buruk	**Sangat Baik**
Kompatibilitas	Sangat Baik	Buruk	Baik	**Baik**
Efisiensi	Buruk	Sangat Baik	Sedang	**Baik**

Berdasarkan analisis di atas, penelitian ini memutuskan untuk mengadopsi **Alt-04 (Kode QR Dinamis Hibrida)**. Keputusan ini diambil karena Alt-04 adalah satu-satunya solusi yang mampu memitigasi risiko keamanan (*anti-cloning*) tanpa mengorbankan ketersediaan layanan saat kondisi jaringan buruk, serta tetap dapat diakses oleh mayoritas perangkat pengguna. Pendekatan ini diharapkan dapat memberikan solusi komprehensif terhadap permasalahan yang dihadapi sistem pertiketan elektronik saat ini, sekaligus memenuhi kebutuhan fungsional dan non-fungsional yang telah diidentifikasi sebelumnya.

BAB IV

DESAIN KONSEP SOLUSI

Bab ini memaparkan rancangan konsep solusi yang diusulkan untuk mengatasi permasalahan keamanan pada sistem *e-ticketing* yang telah diidentifikasi sebelumnya. Pemaparan dilakukan dengan membandingkan model konseptual sistem yang berjalan saat ini dengan model sistem usulan yang menerapkan teknologi *Dynamic Secure QR Code*. Perbandingan ini bertujuan untuk mempertegas perbedaan arsitektur keamanan dan alur data antara kedua sistem.

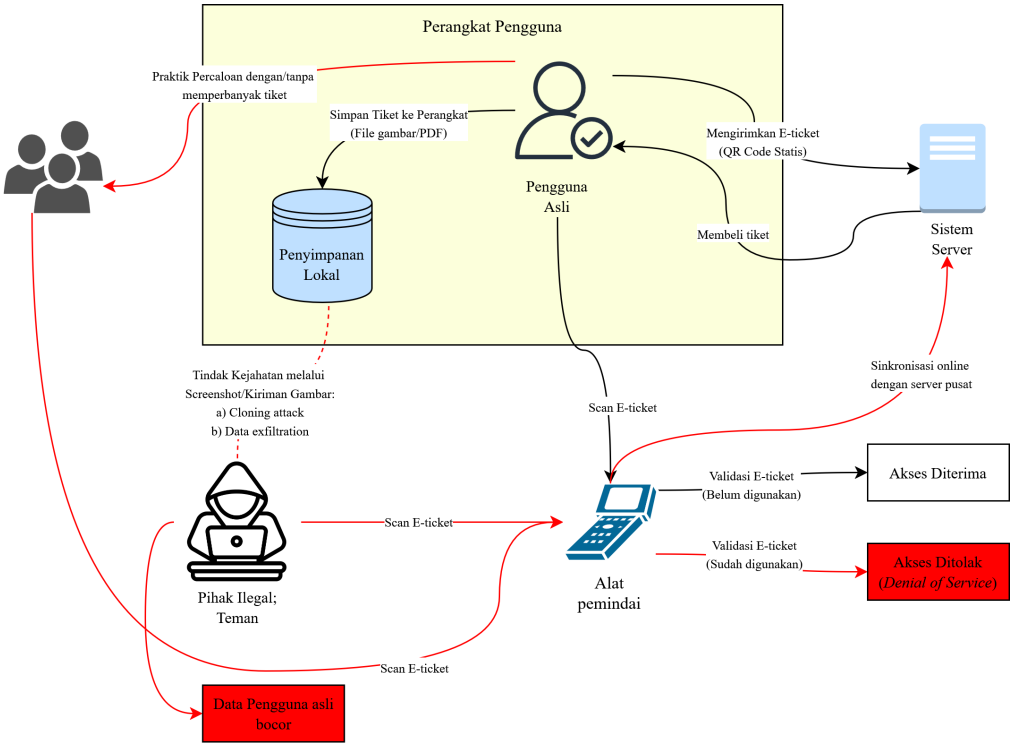
IV.1 Desain Konsep Solusi

Desain konsep solusi digambarkan melalui model konseptual yang memetakan interaksi antara pengguna, perangkat, dan server, serta bagaimana data tiket dikelola. Bagian ini dibagi menjadi dua perspektif: model sistem saat ini (*as-is*) dan model sistem usulan (*to-be*).

IV.1.1 Model Konseptual Sistem Saat Ini

Model sistem saat ini, sebagaimana diilustrasikan pada Gambar IV.1, menunjukkan alur distribusi tiket yang berbasis pada berkas (*file*) statis. Pada model ini, server mengirimkan tiket dalam bentuk gambar kode QR statis atau berkas PDF kepada pengguna. Pengguna kemudian menyimpan berkas tersebut ke dalam penyimpanan lokal perangkat. Kelemahan mendasar dari model ini adalah sifat tiket yang permanen dan mudah dipindahtangankan.

Seperti terlihat pada Gambar IV.1, celah keamanan muncul karena tidak adanya batasan validitas waktu pada gambar tiket, yang memungkinkan terjadinya praktik percaloan, *cloning attack* melalui tangkapan layar (*screenshot*), hingga kebocoran data pengguna asli jika berkas tersebut jatuh ke pihak ilegal. Validasi hanya bergantung pada sinkronisasi *online* dengan server pusat tanpa memverifikasi “kesegaran”



Gambar IV.1 Model Konseptual Sistem Saat Ini

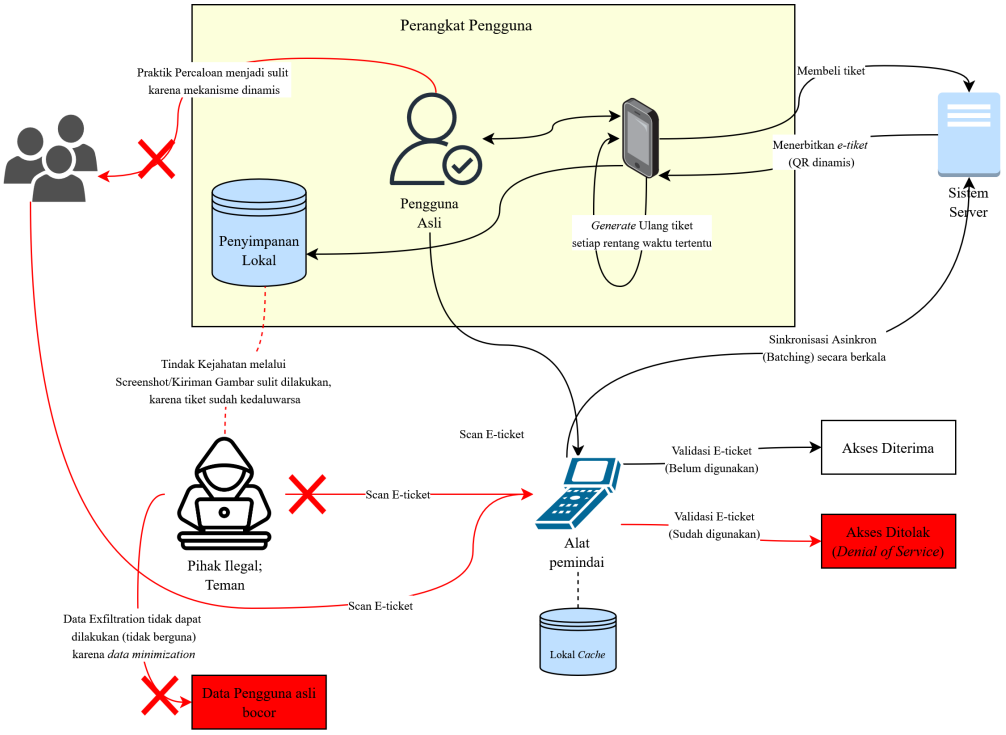
data tiket.

IV.1.2 Model Konseptual Sistem Usulan

Model sistem usulan dirancang untuk menutup celah keamanan tersebut dengan mengubah paradigma perangkat pengguna, dari "penyimpanan tiket" menjadi "pembangkitan tiket". Ilustrasi model usulan dapat dilihat pada Gambar IV.2. Pada model usulan ini, setelah penerbitan tiket pertama kali, server tidak lagi mengirimkan gambar tiket agar pengguna mendapatkan tiket terbaru berdasarkan token dinamis. Pada model ini, diberikan hak akses yang memungkinkan aplikasi pengguna melakukan pembangkitan ulang (*regenerate*) tiket secara mandiri setiap rentang waktu tertentu (dinamis). Proses ini digambarkan dengan alur *looping* pada perangkat pengguna.

Sistem usulan ini secara efektif memutus ancaman sistem lama melalui mekanisme berikut:

a) Pembangkitan Tiket Dinamis: Mekanisme perubahan kode secara terus-menerus menyulitkan praktik percaloan dan penjualan kembali tiket, karena tiket yang dijual saat ini tidak akan valid beberapa detik kemudian.
b) Pembatasan Validitas Waktu (*Time-based Validity*): Tindak kejahatan melalui tangkapan layar (*screenshot*) dapat digagalkan karena gambar tiket akan



Gambar IV.2 Model Konseptual Sistem Usulan

kedaluwarsa secara otomatis dalam hitungan detik (mengikuti siklus TOTP).

c) Minimalisasi Data (*Data Minimization*): Risiko eksfiltrasi data dimitigasi dengan hanya memuat data teknis non-sensitif pada *payload* kode QR, sehingga tidak ada informasi pribadi yang dapat dicuri dari perangkat pengguna.

d) Validasi Mandiri dan Sinkronisasi Asinkron: Alat pemindai dapat melakukan validasi secara *offline* (*stateless*) untuk mencegah kegagalan sistem, didukung dengan pengiriman log data secara berkala (*batching*) yang lebih efisien.

IV.2 Analisis Perbandingan Sistem

Berdasarkan kedua model konseptual di atas, analisis perbandingan antara sistem saat ini dengan solusi yang diusulkan dapat dirangkum dalam aspek-aspek berikut:

1. Mekanisme Pembangkitan Data (*Data Generation*): Sistem saat ini menggunakan mekanisme *Generate Once*, yaitu kode QR dibangkitkan sekali oleh server dan berlaku selamanya. Sebaliknya, sistem usulan menerapkan mekanisme *Continuous Generation*, yaitu aplikasi klien membangkitkan kode baru secara berkala berdasarkan algoritma waktu (*Time-Based*) dan kunci rahasia, sebagaimana ditunjukkan oleh indikator *loop* pada model usulan.
2. Integritas dan Validitas Tiket: Pada sistem lama, validitas tiket hanya bergantung pada ID tiket. Jika ID tersebut belum dipindai, maka tiket dianggap sah,

tanpa mempedulikan siapa yang memegangnya. Pada sistem usulan, validitas diperketat dengan penambahan variabel waktu dan tanda tangan digital. Hal ini memastikan bahwa tiket yang dipindai adalah tiket yang dibangkitkan secara *real-time* oleh aplikasi resmi, bukan hasil duplikasi atau *replay attack*.

3. Manajemen Konektivitas dan Sinkronisasi Data: Sistem saat ini menerapkan model *Synchronous Online Validation*, yaitu setiap pemindaian memerlukan konfirmasi langsung dari server pusat. Hal ini menciptakan ketergantungan fatal terhadap ketersediaan jaringan (*Single Point of Failure*). Sebaliknya, sistem usulan mengadopsi model *Asynchronous Batching* dengan dukungan *Local Cache*. Validasi dapat dilakukan secara mandiri di perangkat pemindai menggunakan data lokal, sementara sinkronisasi status ke server dilakukan secara berkala di latar belakang. Hal ini dapat meminimalisasi risiko kegagalan sistem akibat gangguan jaringan.
4. Mitigasi Risiko Keamanan: Seperti yang ditunjukkan oleh tanda silang merah pada model usulan (Gambar IV.2), sistem baru secara desain memblokir tiga vektor serangan utama:
    a) Pencurian dan Percaloan: Sulit dilakukan karena tidak ada berkas gambar statis yang tersimpan permanen di galeri pengguna untuk dipindahtangankan.
    b) Penggandaan (*Cloning*): Dicegah melalui mekanisme kedaluwarsa yang cepat, membuat salinan tiket (hasil *screenshot*) menjadi tidak berguna saat dipindai (*Denial of Service* bagi pihak ilegal).
    c) Eksfiltrasi Data: Risiko kebocoran data pribadi dimitigasi melalui prinsip *Data Minimization*, dengan cara mengatur *payload* tiket hanya memuat atribut teknis non-sensitif sehingga tidak ada data privasi yang dapat diekstrak oleh pihak ketiga dari kode QR.

Berdasarkan analisis terhadap mekanisme pembangkitan, validitas, manajemen konektivitas, dan mitigasi risiko di atas, terlihat jelas adanya pergeseran paradigma keamanan dari sistem konvensional menuju sistem yang diusulkan. Untuk mempermudah pemahaman mengenai signifikansi perubahan tersebut, ringkasan komparatif antara karakteristik sistem saat ini (*As-Is*) dengan sistem usulan (*To-Be*) disajikan secara terstruktur pada Tabel IV.1. Perbandingan ini menyoroti perbedaan fundamental pada aspek bentuk tiket, masa berlaku, hingga ketergantungan terhadap infrastruktur jaringan.

Tabel IV.1 Perbandingan Sistem Saat Ini dan Sistem Usulan

Kriteria	**Sistem Saat Ini (*As-Is*)**	**Sistem Usulan (*To-Be*)**
Bentuk Tiket	Berkas statis (Gambar/PDF) yang dikirim dan disimpan di perangkat.	Kode dinamis yang dibangkitkan ulang (*regenerated*) pada aplikasi.
Masa Berlaku Visual	Permanen (selama tiket belum dipindai).	Terbatas waktu (*Time-based*, misal: 30 detik) mengikuti algoritma TOTP.
Ketahanan terhadap Penggandaan	Rentan terhadap penyebaran berkas dan tangkapan layar (*screenshot*).	Tahan terhadap *screenshot* karena kode visual akan kedaluwarsa dengan cepat.
Mekanisme Validasi	Validasi tunggal berbasis ID tiket ke *database* pusat.	Validasi berlapis: Verifikasi ID, Tanda Tangan Digital, dan Validasi Kebaruan Tiket.
Ketergantungan Konektivitas	Tinggi (memerlukan sinkronisasi *online* penuh saat pemindaian).	Fleksibel (mendukung validasi *offline* parsial melalui verifikasi kriptografi di sisi pemindai).

IV.3 Perancangan Alur Proses Sistem

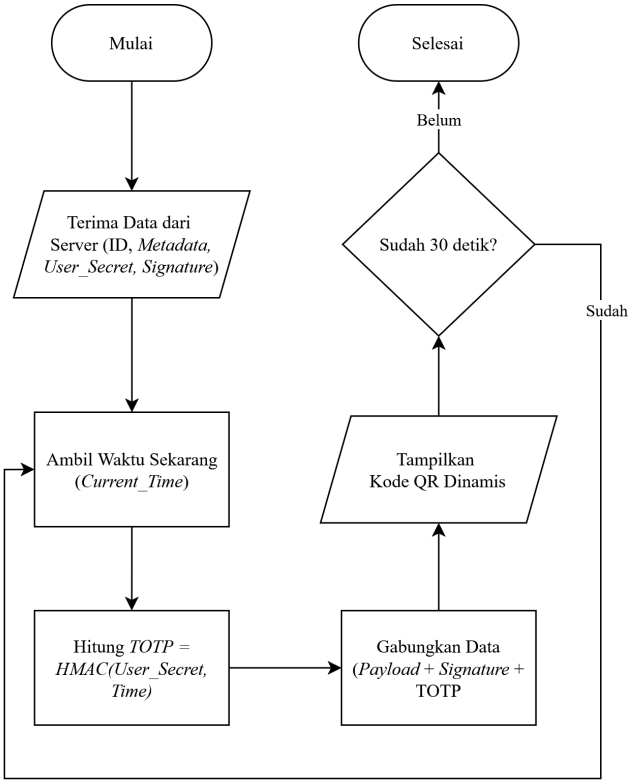
Perancangan alur proses berfokus pada mekanisme pembangkitan tiket dan validasi *stateless* yang memungkinkan verifikasi dilakukan secara *offline* tanpa mengorbankan keamanan. Sistem menerapkan pendekatan *Hybrid Verification* yang menggabungkan Tanda Tangan Digital (untuk integritas data statis) dan TOTP (untuk validitas waktu dinamis).

IV.3.1 Alur Pembangkitan Tiket (Sisi Klien)

Berbeda dengan pendekatan enkripsi penuh, sistem ini menerapkan prinsip *Data Minimization*. Hanya data teknis non-sensitif yang dimasukkan ke dalam *payload* tiket, sementara data pribadi pengguna tetap tersimpan aman di server. Alur logika pembangkitan tiket pada aplikasi pengguna digambarkan pada Gambar IV.3.

Mekanisme pembangkitan tiket yang dijelaskan pada IV.3 meliputi langkah-langkah berikut:

1. Inisiasi Data: Saat pembelian berhasil, server menyusun *payload* data yang hanya berisi informasi non-sensitif (ID Tiket, Jenis Tiket, dan Metadata Area). Data identitas pribadi pengguna (PII) tetap disimpan di server dan tidak disertakan dalam *payload*.
2. Signing & Key Distribution: Server menandatangani *payload* tersebut meng-



Gambar IV.3 Flowchart Proses Pembangkitan Tiket di Sisi Klien

gunakan Kunci Privat Server (untuk integritas). Server juga menurunkan kunci rahasia unik pengguna (`user_secret`) dari `MASTER_SECRET` menggunakan fungsi *Key Derivation* (HMAC). Kunci unik dan tanda tangan digital dikirim ke aplikasi pengguna.

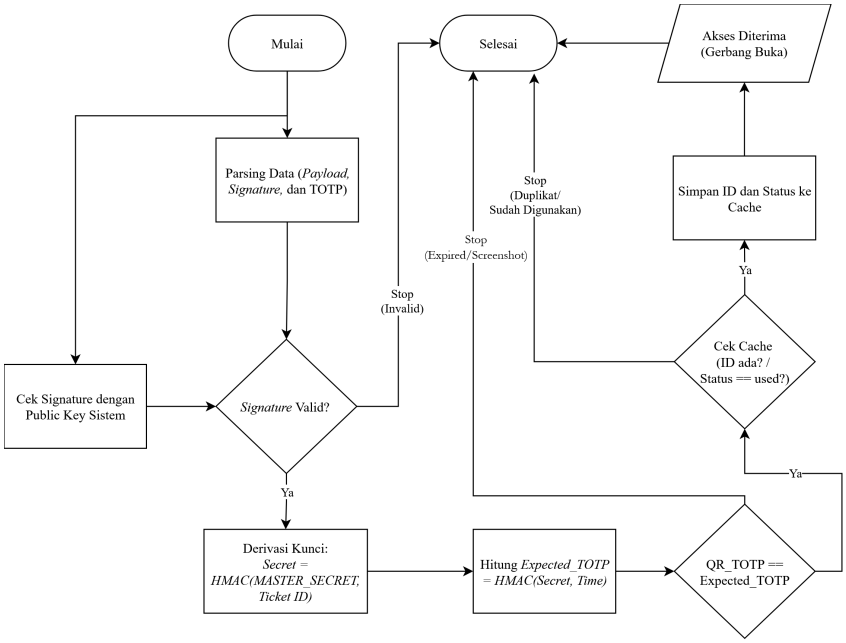
3. Pembangkitan TOTP Lokal: Setiap 30 detik, aplikasi pengguna menghitung kode TOTP menggunakan `user_secret` yang tersimpan aman di perangkat.
4. Visualisasi QR: Aplikasi menggabungkan *Payload* (Statis), Tanda Tangan Digital, dan Kode TOTP (Dinamis) ke dalam satu format QR Code untuk ditampilkan.

IV.3.2 Alur Validasi Tiket (Sisi Pemindai)

Proses validasi dirancang agar dapat berjalan tanpa koneksi internet (*offline-first*) dengan memanfaatkan skema *Key Derivation*. Alur logika validasi pada alat pemindai digambarkan pada Gambar IV.4.

Mekanisme validasi mencakup langkah-langkah berikut:

1. *Parsing* dan Verifikasi Integritas: Pemindai membaca Kode QR dan memisahkan data menjadi *Payload*, *Signature*, dan TOTP. Pemindai memverifikasi



Gambar IV.4 Flowchart Proses Validasi Tiket Stateless

Tanda Tangan Digital menggunakan Kunci Publik Server yang tersimpan di aplikasi. Jika tanda tangan tidak cocok, tiket ditolak (terindikasi dimodifikasi).

2. Derivasi Kunci Mandiri (*Key Derivation*): Jika integritas valid, pemindai melakukan perhitungan ulang kunci rahasia pengguna secara mandiri menggunakan rumus:

$$User\_Secret = HMAC(MASTER\_SECRET, Ticket\_ID) \quad \text{(IV.1)}$$

Hal ini memungkinkan pemindai mengetahui kunci rahasia pengguna tanpa perlu menyimpan basis data kunci seluruh pengguna.

3. Validasi Waktu (TOTP): Menggunakan `User_Secret` hasil derivasi dan waktu internal pemindai, sistem menghitung nilai TOTP yang valid saat itu. Jika nilai TOTP pada QR cocok dengan hasil hitungan, maka tiket dinyatakan asli (*fresh*) dan bukan hasil tangkapan layar lama.
4. Pencegahan Penggunaan Ganda: ID Tiket dicatat dalam penyimpanan lokal (*Local Cache*) pemindai untuk mencegah *replay attack* atau penggunaan berulang dalam sesi yang sama.

BAB V

RENCANA SELANJUTNYA

Bab ini menguraikan peta jalan (*roadmap*) realisasi sistem *Dynamic Secure QR Code* dari tahap perancangan menuju tahap implementasi nyata. Rencana ini mencakup kebutuhan sumber daya teknis, strategi pengujian untuk memvalidasi hipotesis keamanan, serta analisis mitigasi risiko untuk menjamin keberhasilan penyelesaian Tugas Akhir dalam kurun waktu pengembangan yang tersedia.

V.1 Rencana Implementasi

Implementasi sistem akan difokuskan pada pembangunan prototipe fungsional (*Proof of Concept*) yang mencakup dua komponen utama: sisi peladen (*Backend*) untuk logika kriptografi pusat dan sisi klien (*Mobile App*) untuk antarmuka pengguna dan pemindai.

V.1.1 Lingkungan Pengembangan dan Alat

Berdasarkan ketersediaan sumber daya saat ini, spesifikasi lingkungan kerja yang digunakan dirangkum dalam Tabel V.1.

Tabel V.1 Spesifikasi Lingkungan Pengembangan dan Alat

Kategori	**Komponen**	**Spesifikasi / Keterangan**
Perangkat Keras	Komputer Pengembang	Laptop HP Probook 440 G8 (Intel Core i5-1135G7, RAM 16GB, Windows 11 Home).
	Perangkat Uji (*Device*)	Dua unit ponsel pintar Android (Satu sebagai *User Generator*, satu sebagai *Scanner/Validator*).
Perangkat Lunak	Backend Server	Python dengan kerangka kerja **FastAPI** (Kinerja tinggi dan dokumentasi otomatis).

Berlanjut ke halaman berikutnya...

Tabel V.1 Spesifikasi Lingkungan Pengembangan dan Alat (Lanjutan)

Kategori	**Komponen**	**Spesifikasi / Keterangan**
	Database Platform	**Supabase** (PostgreSQL) sebagai layanan *Database-as-a-Service*.
	Mobile Application	**React Native** dengan platform **Expo** (Integrasi kamera dan UI).
	Modul Kriptografi	`pyotp` (TOTP RFC 6238), `cryptography` (Digital Signature), `hashlib/hmac` (Key Derivation).
	Tools Pendukung	Visual Studio Code, Postman (API Testing), dan Git.

V.1.2 Konfigurasi dan Topologi

Implementasi sistem pada tahap awal akan dilakukan menggunakan topologi jaringan lokal (*Local Area Network*). Dalam skema ini, server FastAPI akan dijalankan pada komputer pengembang (*localhost*) yang bertindak sebagai pusat pemrosesan logika. Komputer pengembang dan perangkat ponsel pintar (klien) akan dihubungkan ke dalam satu jaringan Wi-Fi yang sama agar dapat saling berkomunikasi.

Proses pengembangan akan dibagi menjadi dua fase simulasi topologi. Fase pertama adalah pengembangan aktif, yaitu aplikasi pada ponsel terhubung langsung ke server lokal melalui *tunnelling* atau IP lokal untuk pertukaran data secara *real-time*. Fase kedua adalah simulasi kondisi nyata, yaitu ketika perangkat pemindai akan dikondisikan dalam mode "Pesawat" atau tanpa internet. Hal ini dilakukan untuk membuktikan bahwa mekanisme derivasi kunci dan validasi kriptografi tetap dapat berjalan secara mandiri (*offline*) tanpa bergantung pada koneksi terus-menerus ke server pusat.

V.1.3 Estimasi Biaya

Mengingat luaran penelitian ini adalah prototipe perangkat lunak, struktur biaya sangat efisien karena memanfaatkan layanan gratis (*free plan*) dari Supabase untuk basis data dan perangkat keras pribadi yang sudah tersedia. Biaya operasional utama dialokasikan hanya untuk konektivitas internet selama proses pengembangan.

V.2 Desain Pengujian dan Evaluasi

Pengujian bertujuan untuk memverifikasi bahwa logika *Key Derivation* dan *Stateless Validation* berjalan sesuai rancangan di Bab IV serta memenuhi kebutuhan fungsional sistem.

V.2.1 Metode Verifikasi (Unit Testing)

Verifikasi dilakukan secara modular pada kode Python (Backend) untuk memastikan fungsi matematis bekerja dengan benar sebelum diintegrasikan ke aplikasi. Rincian metode verifikasi dapat dilihat pada Tabel V.2.

Tabel V.2 Rencana Verifikasi Unit (Unit Testing)

Unit Uji	**Tujuan dan Prosedur Verifikasi**
Uji Derivasi Kunci	Memastikan fungsi HMAC pada Python menghasilkan *string* kunci yang konsisten dan deterministik untuk setiap ID tiket yang unik.
Uji Pembangkitan TOTP	Memastikan pustaka `pyotp` mampu menghasilkan token 6 digit yang valid sesuai dengan *timestamp* saat ini dan jendela waktu yang ditentukan.
Uji Tanda Tangan Digital	Memastikan mekanisme verifikasi tanda tangan (*Digital Signature*) berfungsi dengan benar, yaitu menerima data asli yang valid dan menolak data yang telah dimodifikasi (integritas data), meskipun perubahan hanya sebesar 1 byte.

V.2.2 Metode Validasi (Functional Testing)

Validasi dilakukan menggunakan metode *Black Box Testing* melalui aplikasi React Native untuk membuktikan keandalan sistem di lapangan. Skenario uji utama meliputi:

Tabel V.3 Rencana Skenario Pengujian Fungsional

Skenario	**Prosedur Uji**	**Hasil yang Diharapkan**
Validasi Normal	Memindai tiket valid dalam jendela waktu 30 detik yang tepat saat koneksi tersedia.	Akses Diterima.
Validasi Offline	Mematikan koneksi internet pada HP Pemindai, lalu memindai tiket valid.	Akses Diterima (Membuktikan fitur *Key Derivation* bekerja tanpa server).
Uji Kedaluwarsa	Mengambil *screenshot* tiket, menunggu 1 menit, lalu memindai hasil *screenshot* tersebut.	Akses Ditolak (Token Expired/Invalid).
Uji Replay/Duplikasi	Memindai tiket yang sama dua kali berturut-turut pada pemindai yang sama dalam waktu singkat.	Akses Ditolak pada percobaan kedua (Terdeteksi di *Local Cache* aplikasi).
Uji Integritas	Memodifikasi *payload* QR Code (misal: mengganti ID Tiket secara manual pada generator QR pihak ketiga) lalu memindainya.	Akses Ditolak (Signature Invalid).

V.2.3 Evaluasi Kinerja

Selain fungsi keamanan, kinerja sistem akan dievaluasi berdasarkan responsivitas aplikasi. Target capaian adalah proses validasi di sisi pemindai (mulai dari pembacaan kamera hingga keputusan Buka/Tutup) harus terjadi di bawah 2 detik agar layak digunakan secara operasional.

V.3 Analisis Risiko dan Mitigasi

Dalam pelaksanaan penelitian ini, teridentifikasi beberapa risiko teknis yang dapat menghambat pencapaian tujuan. Analisis risiko beserta strategi mitigasinya dijabarkan sebagai berikut:

1. Risiko Desinkronisasi Waktu (*Clock Drift*): Mengingat validasi dilakukan secara *offline*, perangkat pemindai sepenuhnya bergantung pada referensi jam

internalnya. Risiko muncul apabila terdapat perbedaan waktu yang signifikan antara jam pada perangkat pemindai dan perangkat pengguna, yang dapat mengakibatkan tiket valid dianggap kedaluwarsa oleh sistem. Sebagai strategi mitigasi, sistem akan mengimplementasikan toleransi jendela waktu (*interval window*) pada konfigurasi pustaka `pyotp` (misalnya mengizinkan validasi ± 1 langkah waktu atau toleransi 30 detik sebelum dan sesudah waktu server) guna mengakomodasi perbedaan waktu (*drift*) yang wajar antar-perangkat keras.

2. Risiko Ketergantungan Supabase (Konektivitas Dev): Supabase merupakan layanan berbasis awan (*cloud*), sehingga terdapat risiko gangguan akses ke manajemen data pengguna apabila koneksi internet selama proses pengembangan terputus. Untuk memitigasi ketergantungan ini, proses pengembangan akan memanfaatkan fitur *Local Development* yang disediakan oleh Supabase CLI untuk menjalankan emulasi basis data secara lokal. Selain itu, strategi manajemen tugas akan disesuaikan dengan tetap memfokuskan pengerjaan pada logika *offline* di sisi aplikasi React Native ketika konektivitas jaringan tidak tersedia.
3. Risiko Keterbatasan Kamera Perangkat Uji: Kamera ponsel dengan spesifikasi rendah berpotensi mengalami kesulitan dalam memindai QR Code dinamis, terutama jika densitas data terlalu tinggi atau kondisi pencahayaan lingkungan kurang memadai. Risiko ini dimitigasi dengan cara mengoptimalkan densitas QR Code melalui prinsip *Data Minimization*, yaitu menjaga muatan (*payload*) data tetap berupa *string* yang ringkas. Selain itu, sistem akan menggunakan tingkat koreksi kesalahan (*Error Correction Level*) yang moderat (Level M) untuk menyeimbangkan antara ketahanan kode terhadap kerusakan dan kemudahan pembacaan oleh sensor kamera standar.

DAFTAR PUSTAKA

Alsuhibany, Suliman A. 2025. "Innovative QR Code System for Tamper-Proof Generation and Fraud-Resistant Verification". *Sensors* 25 (13). ISSN: 1424-8220. https://doi.org/10.3390/s25133855. https://www.mdpi.com/1424-8220/25/13/3855.

Amazon Web Services. 2017. *Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region.* Laporan Insiden Teknis.

Bafandehkar, Mohsen, Sharifah Md Yasin, Ramlan Mahmod, dan Zurina Hanapi. 2013. "Comparison of ECC and RSA Algorithm in Resource Constrained Devices". *IT Convergence and Security 2012,* 1–7.

Berma, Raienheart Boas. 2023. "Analisis Kerugian Penonton Konser (Coldplay) Ditinjau Dari Hukum Positif Indonesia". Badan Pembinaan Hukum Nasional (BPHN). Diakses pada 8 Desember 2025. https://rechtsvinding.bphn.go.id/?page=artikel&berita=856.

Chen, Fisher Chia-Yu. 2007. "Passenger use intentions for electronic tickets on international flights". *Journal of Air Transport Management* 13 (2): 110–115. https://doi.org/10.1016/j.jairtraman.2006.09.004.

Diveranta, Aditya, Fajar Ramadhan, Johanes Galuh Bimantara, dan Harry Susilo. 2025. "Jejak Transaksi Penipuan Tiket Konser Disamarkan (5)". Diakses pada 8 Desember 2025. https://www.kompas.id/artikel/jejak-transaksi-penipuan-tiket-konser-disamarkan.

Ghomi, Einollah Jafarnejad, Amir Masoud Rahmani, dan Nooruldeen Nasih Qader. 2017. "Load-balancing algorithms in cloud computing: A survey". *Journal of Network and Computer Applications* 88:50–71. https://doi.org/10.1016/j.jnca.2017.04.007.

Kurniawan, Hery. 2024. “Banyak Penonton Tidak Bertiket Masuk SUGBK saat Timnas Indonesia Vs Jepang: Malah yang Punya Tiket Tidak Dapat Tempat Duduk”. Diakses pada 29 Oktober 2025.

Labs, Cockroach. 2023. *Technical takeaways from the Taylor Swift/Ticketmaster meltdown.* https://www.cockroachlabs.com/blog/taylor-swift-ticketmaster-meltdown/. Diakses: 2025.

Lever, Kirsty E, Madjid Merabti, dan Kashif Kifayat. 2013. “Single points of failure within systems-of-systems”. Dalam *Proceedings of the 14th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet),* 1–6.

Lübeck, Rafael Mendes, Milton Luiz Wittmann, dan Luciana Flores Battistella. 2012. “Electronic Ticketing System As a Process of Innovation”. *Journal of Technology Management & Innovation* 7 (1): 18–29. ISSN: 0718-2724. https://doi.org/10.4067/S0718-27242012000100002.

Pamela, Dyah Ayu. 2023. “Tiket Konser Coldplay di Jakarta 2023 Dijual Calo Berkali-kali Lipat hingga Rp22 Juta di Marketplace”. Diakses pada 29 Oktober 2025.

Ramachandra, Karthik, Mahendra Chavan, Ravindra Guravannavar, dan S. Sudarshan. 2015. “Program Transformations for Asynchronous and Batched Query Submission”. *IEEE Transactions on Knowledge and Data Engineering* 27 (2): 531–544. https://doi.org/10.1109/TKDE.2014.2334302.

Shin, Dong-Hee, Jaemin Jung, dan Byeng-Hee Chang. 2012. “The psychology behind QR codes: User experience perspective”. *Computers in Human Behavior* 28 (4): 1417–1426. ISSN: 0747-5632. https://doi.org/https://doi.org/10.1016/j.chb.2012.03.004. https://www.sciencedirect.com/science/article/pii/S0747563212000702.

Sommerville, Ian. 2016. *Software Engineering.* 10th edisi. Global Edition. Harlow, England: Pearson Education Limited. ISBN: 978-1-292-09613-1.

Stallings, William. 2022. *Cryptography and Network Security: Principles and Practice.* 8th edisi. Global Edition. Pearson Education Limited. ISBN: 978-1-292-43749-1.

Sung, Siwon, Joonghwan Lee, Jinmok Kim, Jongho Mun, dan Dongho Won. 2015. "Security analysis of mobile authentication using QR-codes". Dalam *Computer Science & Information Technology (CS & IT),* 151–160. AIRCC Publishing Corporation. https://doi.org/10.5121/csit.2015.51612.

Tang, Bin, Himanshu Gupta, dan Samir Das. 2006. "Benefit-based Data Caching in Ad Hoc Networks". Dalam *Proceedings of the 2006 IEEE International Conference on Network Protocols,* 208–217. https://doi.org/10.1109/ICNP.2006.320214.

Tiwari, Sumit. 2016. "An Introduction to QR Code Technology". Dalam *2016 International Conference on Information Technology (ICIT),* 39–44. https://doi.org/10.1109/ICIT.2016.021.

Yanuarafi, Arisal. 2023. "Perbandingan QR Code Statis dan QR Code Dinamis dalam Pengambilan Absen Pegawai di Lingkungan Universitas Bung Hatta". *Al-Ma'arif: Jurnal Ilmu Perpustakaan dan Informasi Islam* 3 (2). ISSN: 0740-8188. https://doi.org/10.37108/almaarif.v3i2.1289.