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 16 Desember 2025

Pembimbing

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

NIP. 197203262008011014

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE

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 QR Code statis. Pada model ini, data tiket seperti identitas pengguna atau tautan validasi, dienkode secara langsung ke dalam pola matriks citra. Karakteristik fundamental dari QR Code 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 QR Code 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 QR Code 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 QR Code statis tidak lagi memadai. Diperlukan sebuah pendekatan komprehensif untuk menjamin integritas transaksi dan data. Berdasarkan analisis masalah tersebut, sebuah sistem *e-ticket* yang ideal harus memiliki tiga karakteristik pertahanan utama. Pertama, tiket harus bersifat dinamis (*dynamic*) menggunakan mekanisme pembangkitan QR Code yang berubah secara berkala berbasis waktu, sehingga tangkapan layar menjadi tidak valid setelah durasi tertentu (Sung dkk. 2015). Kedua, tiket harus menjamin kerahasiaan (*confidentiality*) melalui enkripsi muatan data (*payload*) untuk melindungi privasi pengguna dari pembacaan data sembarangan serta risiko eksfiltrasi data dari penyimpanan lokal (Sung dkk. 2015). Ketiga, tiket harus bersifat aman (*secure*) menggunakan mekanisme tanda tangan digital (*digital signature*) yang menjamin aspek nirsangkal (*non-repudiation*), untuk memastikan tiket diterbitkan oleh otoritas yang sah dan

tidak dimodifikasi.

Oleh karena itu, penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem *e-ticket* yang mengusung konsep *Dynamic Secure QR Code*. Urgensi penelitian ini difokuskan pada sektor hiburan dan olahraga skala besar, mengingat sektor ini memiliki risiko kerugian tertinggi akibat manipulasi tiket. Melalui implementasi sistem ini, diharapkan tercipta ekosistem pertiketan yang lebih sehat yang memberikan manfaat ganda: konsumen mendapatkan jaminan perlindungan hak akses dan data pribadi, sementara penyelenggara acara dapat memitigasi kebocoran pendapatan (*revenue leakage*) akibat tiket palsu. Penelitian ini akan berfokus pada pengembangan prototipe sistem yang mampu membangkitkan dan memvalidasi tiket dengan arsitektur keamanan berlapis tersebut.

I.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, teridentifikasi adanya kelemahan fundamental pada arsitektur *e-ticket* berbasis QR Code 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* yang mengintegrasikan konsep *Dynamic Secure QR Code* untuk menjamin aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan nirsangkal (*non-repudiation*)?
2. Bagaimana mekanisme pembangkitan dan validasi tiket menggunakan kombinasi algoritma enkripsi, pembangkitan kode dinamis berbasis waktu, dan Tanda Tangan Digital untuk mencegah pemalsuan dan modifikasi tiket.
3. Bagaimana efektivitas penerapan kode dinamis berbasis waktu dalam memitigasi serangan penggandaan tiket (*cloning*) melalui tangkapan layar (*screenshot*) dan serangan putar ulang (*replay attack*) dibandingkan dengan sistem statis?

I.3 Tujuan

Mengacu pada rumusan masalah yang telah dipaparkan, tujuan utama dari penelitian ini adalah:

1. Merancang arsitektur sistem *e-ticket* yang mampu memenuhi standar keamanan informasi, meliputi aspek kerahasiaan data (*confidentiality*), integritas data (*integrity*), dan nirsangkal (*non-repudiation*).
2. Mengimplementasikan prototipe (*proof-of-concept*) sistem yang dapat mem-

bangkitkan dan memvalidasi tiket menggunakan kombinasi enkripsi muatan, kode dinamis berbasis waktu, dan tanda tangan digital (*digital signature*).
3. Mengevaluasi efektivitas sistem yang diusulkan melalui serangkaian pengujian keamanan untuk membuktikan kemampuannya dalam memitigasi serangan penggandaan tiket (*cloning*) dan pemalsuan tiket (*forgery*).

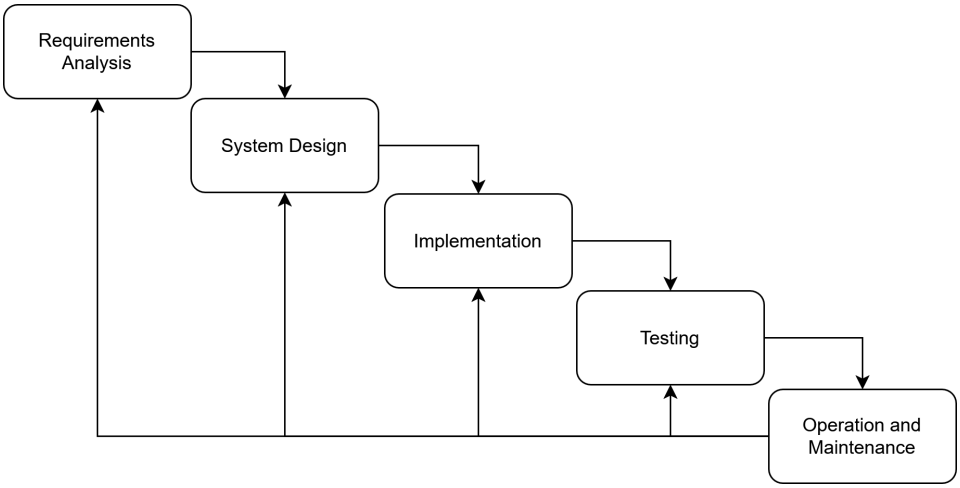
I.4 Batasan Masalah

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 keamanan, yaitu proses pembangkitan (*generation*) dan validasi (*validation*) *Dynamic Secure QR Code*, tanpa membahas aspek antarmuka pengguna (UI-/UX) secara mendalam.
2. Penelitian ini tidak akan membangun sistem *e-commerce* atau *marketplace* penjualan tiket yang utuh. Fitur pendukung seperti manajemen akun pengguna, gerbang pembayaran (*payment gateway*), dan manajemen acara (*event management*) berada di luar lingkup penelitian.
3. Luaran sistem yang dibangun berupa prototipe (*proof-of-concept*) yang bertujuan untuk mendemonstrasikan kelayakan logika keamanan, bukan sebagai aplikasi skala produksi yang siap dirilis secara komersial (siap pakai).
4. Implementasi teknis prototipe akan dikembangkan menggunakan bahasa pemrograman Python dengan memanfaatkan pustaka (*library*) kriptografi standar dan modul QR Code yang relevan.
5. Penelitian tidak mencakup perancangan perangkat keras (*hardware*) pemindai khusus. Proses pemindaian dan validasi diasumsikan dilakukan menggunakan perangkat lunak pada ponsel pintar berbasis kamera.

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* pada acara berskala besar di media sosial, serta mengumpulkan data sekunder dari sumber kredibel, seperti laporan PPATK dan pemberitaan media massa terkait modus kejahatan tiket. Selain itu, dilakukan studi literatur terhadap penelitian terdahulu dan standar teknis terkait algoritma kriptografi untuk menentukan kombinasi teknologi yang tepat, seperti mekanisme *Time-based One-Time Password* (TOTP) dan Tanda Tangan Digital, untuk menjawab permasalahan keamanan yang telah dirumuskan.
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 dengan merancang diagram arsitektur yang menggambarkan interaksi antara sisi klien (aplikasi seluler) dan sisi server (*backend*). Kedua, dilakukan perancangan logika dan alur data melalui pembuatan diagram alur (*Flowchart*) dan diagram aktivitas (*Activity Diagram*) untuk mendetailkan algoritma pembangkitan tiket yang melibatkan proses enkripsi *payload* dan penandatanganan digital. Terakhir, tahap ini meliputi perancangan antarmuka pengguna (*User Interface*) untuk aplikasi seluler guna memastikan fitur pemindaian dan tampilan tiket dapat digunakan dengan baik.

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

   Tahapan ini bertujuan untuk merealisasikan rancangan desain menjadi unit program yang fungsional. Implementasi dilakukan dengan mengembangkan aplikasi seluler (*mobile app*) menggunakan kerangka kerja **React Native/Expo** yang berfungsi sebagai antarmuka pengguna dan alat pemindai QR Code. Aplikasi ini akan terintegrasi dengan logika keamanan inti yang dibangun menggunakan bahasa pemrograman Python, yang bertugas menangani proses kriptografi, pembangkitan token dinamis, dan validasi tanda tangan digital di sisi *backend*.

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

   Setelah prototipe berhasil dibangun, tahap pengujian dilakukan untuk memverifikasi keandalan sistem dan memastikannya bebas dari cacat logika keamanan. Pengujian akan dilakukan menggunakan skenario *Security Testing* yang mensimulasikan serangan nyata, seperti uji ketahanan terhadap serangan tangkapan layar (*screenshot*) dan uji deteksi pemalsuan tiket. Tujuannya adalah untuk membuktikan secara empiris bahwa sistem mampu menolak tiket yang tidak sah atau tiket yang telah dimodifikasi.

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, akan didokumentasikan secara sistematis. Tahapan ini juga mencakup penarikan kesimpulan berdasarkan hasil pengujian untuk menjawab rumusan masalah yang telah ditetapkan di awal penelitian 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* (QR) Code

II.2.1 Sejarah dan Prinsip Kerja

Quick Response Code (QR Code) 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 QR Code 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.

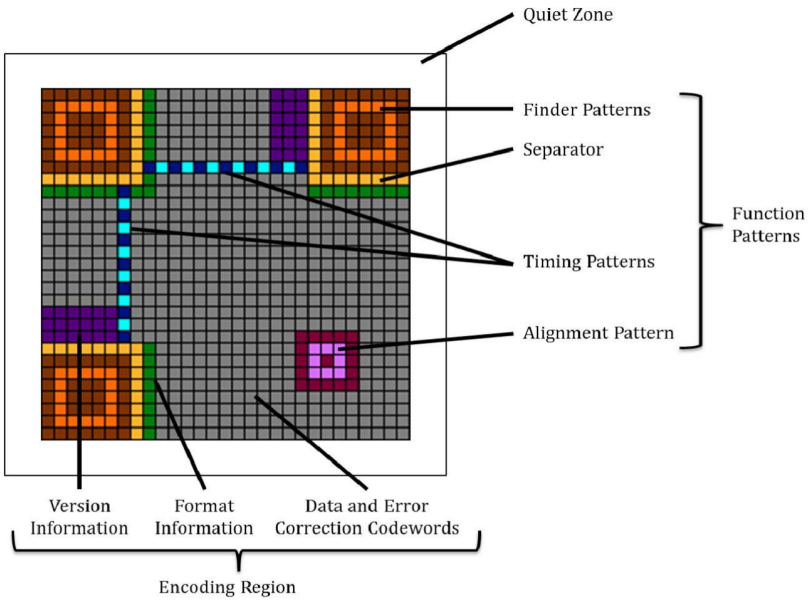
Berbeda dengan kode batang (*barcode*) satu dimensi yang hanya menyimpan data secara horizontal, QR Code mengodekan informasi dalam dua arah, yaitu vertikal dan horizontal. Struktur dua dimensi ini memungkinkan QR Code memiliki densitas informasi yang jauh lebih tinggi dan kapasitas penyimpanan yang 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 QR Code

Kemampuan QR Code untuk dibaca dengan cepat dan akurat (*high-speed reading*) didukung oleh strukturnya yang unik. Berdasarkan spesifikasi teknis yang dijelaskan oleh Tiwari (2016), setiap simbol QR Code 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 QR Code dapat dilihat pada Gambar II.1, dan untuk rincian dari *function patterns* dijelaskan sebagai berikut:



Gambar II.1 Struktur QR Code (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 QR Code 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 QR Code Statis vs. Dinamis

Dalam implementasi sistem informasi, QR Code dikategorikan berdasarkan sifat data yang dikandungnya. Pemahaman terhadap perbedaan ini sangat krusial 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 QR Code berubah total setiap interval waktu tertentu. Sung dkk. (2015) menyoroti pentingnya mekanisme kedaluwarsa (*expiration*) pada QR Code 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 QR Code statis. Berikut adalah analisis mengenai metode serangan tersebut:

II.3.2.1 Serangan Penggandaan (*Cloning Attack*)

Serangan ini merupakan metode utama untuk melakukan penipuan tiket. Pelaku menyalin citra QR Code 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.

II.3.2.2 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.

II.3.2.3 Eksfiltrasi Data (*Data Exfiltration*)

Serangan ini menargetkan kerahasiaan data pengguna. Sung dkk. (2015) menjelaskan bahwa data kredensial yang disimpan tanpa enkripsi di penyimpanan lokal perangkat rentan dicuri oleh *malware*. Informasi yang dicuri ini kemudian dapat digunakan oleh penyerang untuk merekonstruksi tiket valid atau melakukan pencurian

identitas pengguna.

II.4 Landasan Teori Kriptografi untuk Solusi

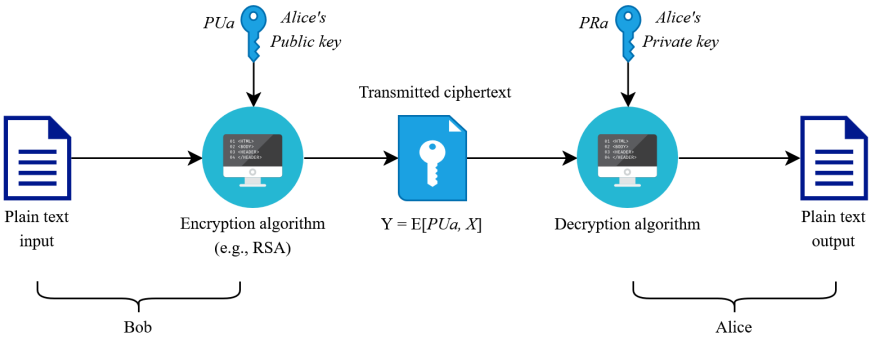
Solusi keamanan yang diusulkan dalam penelitian ini, yaitu *Dynamic Secure QR Code*, dibangun di atas fondasi algoritma kriptografi modern. Subbab ini akan menguraikan konsep teoretis dari teknologi kriptografi yang digunakan, meliputi kriptografi asimetris sebagai kerangka kerja utama, tanda tangan 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*)

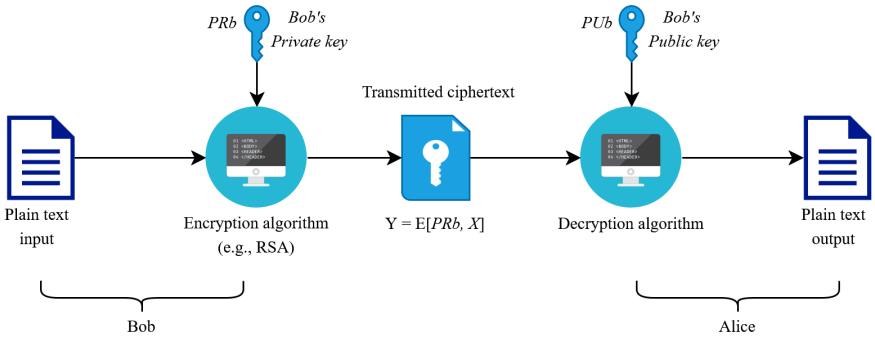
Kriptografi asimetris, atau sering disebut kriptografi kunci publik, merupakan konsep fundamental dalam keamanan informasi modern yang diperkenalkan untuk mengatasi kelemahan distribusi kunci pada kriptografi simetris. Stallings (2022) menjelaskan bahwa skema ini menggunakan dua kunci berbeda yang saling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



(a) Enkripsi Kunci Publik (Kerahasiaan)



(b) Enkripsi Kunci Privat (Autentikasi)

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

Mekanisme kerja sistem ini didasarkan pada fungsi satu arah (*one-way function*). Dalam skenario menjaga kerahasiaan (*confidentiality*), pengirim menggunakan kunci publik penerima untuk mengenkripsi pesan, dan hanya penerima yang memiliki kunci privat pasangannya yang dapat mendekripsi pesan tersebut (Gambar II.2a). Sebaliknya, dalam skenario autentikasi, kunci privat digunakan untuk mengenkripsi (menandatangani) pesan, yang kemudian dapat diverifikasi oleh siapa saja menggunakan kunci publik (Gambar II.2b).

Pada pengerjaan tugas akhir ini, secara spesifik akan memanfaatkan algoritma *Elliptic 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. Sebagai ilustrasi, kunci ECC sebesar 160-bit menawarkan tingkat keamanan yang setara dengan kunci RSA 1024-bit. Karak-

teristik ini menjadikan ECC sangat ideal untuk diimplementasikan pada perangkat dengan sumber daya komputasi terbatas seperti ponsel pintar dalam sistem *e-ticket*.

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 yang beroperasi pada grup kurva eliptik.

II.4.3 *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:

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

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:

$$T = \lfloor \frac{CurrentTime - T0}{X} \rfloor \tag{II.2}$$

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:

$$TOTP = HOTP(K, T) \tag{II.3}$$

Penggunaan TOTP menjamin bahwa *payload* kode QR akan selalu berubah secara periodik mengikuti waktu server sehingga 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 menyimpan data kredensial tiket yang telah diverifikasi atau data kunci publik yang diperlukan sehingga memungkinkan proses validasi tetap berjalan instan (*low latency*) tanpa ketergantungan penuh pada koneksi internet setiap saat.

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 QR Code 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 QR Code dinamis.

II.6.1 Sistem QR Code 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 QR Code 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 menyisipkan pola keamanan unik (yang berbeda untuk setiap pasar) ke dalam citra QR Code 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 QR Code 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. Dalam ekosistem *e-ticket*, ancaman utama adalah duplikasi melalui tangkapan layar (*screenshot*) yang menghasilkan salinan digital identik secara bit-per-bit, tanpa degradasi fisik yang dapat dideteksi oleh model CNN tersebut. Oleh karena itu, solusi berbasis analisis citra statis seperti yang ditawarkan Alsuhibany perlu dilengkapi dengan mekanisme dinamis (perubahan konten) untuk mematahkan validitas salinan digital tersebut.

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

Penelitian yang dilakukan oleh Sung dkk. (2015) menyajikan analisis keamanan komprehensif terhadap sistem autentikasi yang menggunakan QR Code pada perangkat seluler. Berbeda dengan pandangan umum yang menganggap QR Code 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 QR Code 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 oleh enkripsi yang memadai. Selain itu, penelitian ini juga membahas ancaman lain seperti penyadapan pesan jaringan (*network eavesdropping*) dan pengungkapan algoritma internal melalui teknik rekayasa balik (*reverse engineering*).

Sebagai usulan mitigasi terhadap implementasi perangkat lunak, Sung dkk. (2015) mengusulkan kerangka kerja implementasi aman (*secure implementation*) yang mencakup beberapa lapisan pertahanan. Rekomendasi utamanya meliputi penerapan mekanisme kedaluwarsa (*expiration*) untuk mencegah serangan putar ulang, enkripsi data penyimpanan untuk mencegah eksfiltrasi, serta pengaburan kode (*code obfuscation*) untuk mempersulit analisis algoritma oleh penyerang. Penelitian tugas akhir ini akan mengadopsi beberapa rekomendasi tersebut dengan cara mengimplementasikan algoritma TOTP untuk manajemen kedaluwarsa otomatis dan enkripsi asimetris pada *payload* tiket guna melindungi data dari risiko eksfiltrasi dan manipulasi.

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

Dalam konteks implementasi sistem autentikasi kehadiran, Yanuarafi (2023) melakukan studi komparatif antara penggunaan QR Code 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 QR Code 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 untuk sistem yang membutuhkan manajemen absensi yang baik.

Meskipun penelitian ini berhasil membuktikan keunggulan konsep dinamis, fokus

utamanya terletak pada fungsionalitas aplikasi presensi dan pencegahan berbagi kode secara sederhana. Penelitian tersebut belum membahas mekanisme perlindungan integritas data secara kriptografis, seperti penggunaan tanda tangan digital (*digital signature*), untuk menjamin bahwa data dinamis yang dihasilkan benar-benar berasal dari otoritas yang sah dan tidak dimanipulasi oleh pihak ketiga selama proses transmisi. Celah inilah yang akan dilengkapi oleh penelitian Tugas Akhir ini melalui arsitektur *Dynamic Secure QR Code*.

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 dinamis untuk mencegah serangan penggandaan, (2) aspek kerahasiaan untuk melindungi data privasi pengguna, 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, enkripsi asimetris (ECC) yang efisien untuk perangkat seluler (Bafandehkar dkk. 2013), dan tanda tangan digital dalam satu sistem yang padu. 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

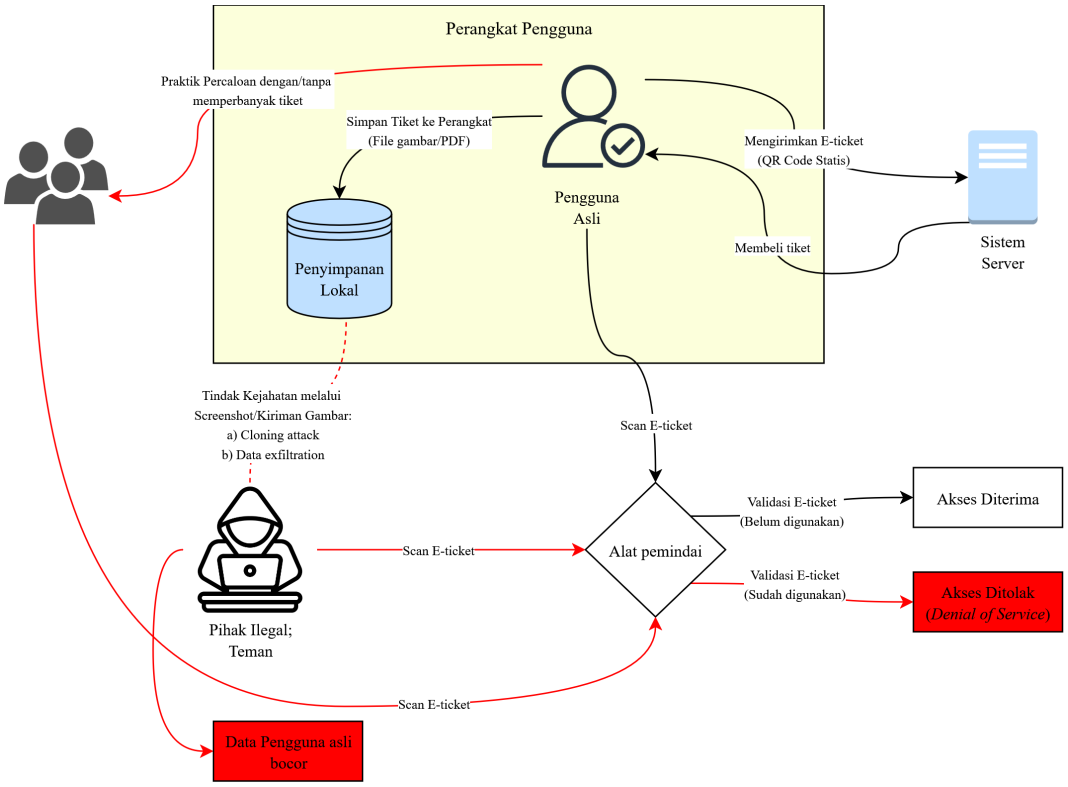
Peneliti	**Fokus Penelitian**	**Dinamis**	**Rahasia**	**Integritas**
Sung dkk. (2015)	Analisis kerentanan autentikasi *mobile*	Saran	Saran	-
Alsuhibany (2025)	*Watermarking* digital pada media cetak	Tidak	Tidak	Ya
Yanuarafi (2023)	Perbandingan presensi statis vs dinamis	Ya	Tidak	-
Penelitian Ini	**Sistem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

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 enkripsi, data ini rentan dicuri (*data exfiltration*) dan disalahgunakan untuk rekayasa sosial atau penipuan.
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 identitas pengguna, kunci rahasia (*secret key*), dan tanda tangan digital, lalu mendistribusikannya secara aman ke perangkat pengguna sebagai inisialisasi awal.
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.
FR-03	Enkripsi *Payload*	Sistem dapat mengenkripsi informasi sensitif pengguna di dalam muatan kode QR menggunakan algoritma kriptografi (misalnya ECC) sehingga data tidak dapat dibaca secara langsung dalam format teks biasa (*plaintext*) oleh pihak tidak berwenang.
FR-04	Integritas Data Tiket	Sistem dapat menyertakan mekanisme penandatanganan digital pada data identitas tiket untuk menjamin keaslian penerbit dan memastikan informasi detail tiket tidak dimodifikasi, yang dapat diverifikasi meskipun dalam kondisi *offline*.

Bersambung ke halaman berikutnya

Tabel III.1 Daftar Kebutuhan Fungsional Sistem (lanjutan)

Kode	Kebutuhan Fungsional	Deskripsi
FR-05	Verifikasi Keaslian dan Dekripsi Tiket	Aplikasi pemindai (*Scanner*) dapat memverifikasi tanda tangan digital dan mendekripsi muatan tiket secara lokal 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 antara perangkat pengguna dan alat pemindai (*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*) di gerbang yang sama saat mode *offline*.
FR-08	Sinkronisasi Asinkron (*Batching*)	Sistem mendukung pengiriman data log kehadiran secara berkala (*batching*) dari pemindai ke server pusat di latar belakang (*background process*) 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 algoritma kriptografi pada muatan (*payload*) kode QR untuk menjamin kerahasiaan data privasi pengguna serta memastikan integritas tiket terhadap upaya pemalsuan maupun serangan komputasi.
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 demi kelancaran antrean (latensi rendah).
NFR-03	Ketersediaan (*Availability*)	Fitur validasi tiket utama (pembangkitan token dinamis, verifikasi tanda tangan digital, dan dekripsi *payload*) 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 dan layar standar, guna menjamin aksesibilitas luas.

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 menggunakakan pendekatan visual dengan memberi *watermarking* 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: QR Code 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, logika pembangkitan token dipindahkan ke sisi perangkat pengguna (*client-side*) menggunakan algoritma *Time-based One-Time Password* (TOTP) yang menjadikan kode QR berubah secara berkala berdasarkan waktu lokal perangkat. Untuk menjamin keamanan data, muatan kode QR dilengkapi dengan tanda

tangan digital (*digital signature*) dan enkripsi asimetris. Keunggulan strategis dari pendekatan ini adalah eliminasi ketergantungan terhadap koneksi internet saat proses validasi berlangsung. Alat pemindai dapat memverifikasi keaslian tiket secara lokal menggunakan algoritma kriptografi tanpa perlu menghubungi server pusat sehingga sistem tetap berjalan lancar meskipun jaringan seluler di lokasi acara mengalami gangguan. Meskipun implementasinya memiliki tantangan kompleksitas yang lebih tinggi—khususnya dalam manajemen kunci kriptografi dan sinkronisasi waktu—solusi ini menawarkan keseimbangan terbaik antara keamanan (*anti-cloning*) dan ketersediaan layanan (*availability*) yang krusial untuk operasional acara berskala besar.

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 (*cloning*), pemalsuan data, dan pencurian identitas. Bobot penilaian ini adalah yang tertinggi mengingat maraknya kasus penipuan tiket.
2. Ketersediaan (*Availability*): Kemampuan sistem untuk tetap beroperasi secara fungsional (dapat dibuka dan dipindai) dalam kondisi infrastruktur jaringan yang buruk atau terputus (*offline/blackout*).
3. Kompatibilitas (*Accessibility*): Tingkat dukungan terhadap ragam perangkat pengguna. Solusi 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 *Watermarking*) 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) merupakan standar industri saat ini yang cukup aman. Namun, solusi ini memiliki risiko nilai ketersediaan yang sangat buruk (*Critical Risk*). Dalam skenario kerumunan massal, saturasi jaringan seluler adalah kejadian yang hampir pasti. 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. Meskipun kompleksitas pengembangannya lebih tinggi, pendekatan ini mencapai nilai Keamanan yang setara dengan Alt-03 (melalui TOTP dan Enkripsi) namun dengan nilai ketersediaan (*availability*) yang jauh lebih tinggi karena kemampuan operasi *offline*. Kompatibilitas juga terjaga karena tetap menggunakan antarmuka optik (layar dan kamera) yang tersedia di semua ponsel pintar.

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

Ilustrasikan desain konsep solusi dalam bentuk model konseptual dan penjelasan secara ringkas, beserta perbedaannya dengan sistem saat ini. Ilustrasi harus dapat dibandingkan (*before* and *after*). Karena masih berupa proposal, bab ini hanya berisi gambar desain konsep solusi tersebut dan penjelasan perbandingannya dengan gambar sistem yang ada saat ini (yang tergambar di awal Bab III).

BAB V

RENCANA SELANJUTNYA

Jelaskan secara detail langkah-langkah rencana selanjutnya, hal-hal yang diperlukan atau akan disiapkan, dan risiko dan mitigasinya, yang meliputi:

1. Rencana implementasi, termasuk alat dan bahan yang diperlukan, lingkungan, konfigurasi, biaya, dan sebagainya.
2. Desain pengujian dan evaluasi, misalnya metode verifikasi dan validasi.
3. Analisis risiko dan mitigasi, misalnya tindakan selanjutnya jika ada yang tidak berjalan sesuai rencana.

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.

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.

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.