BAB II

LANDASAN TEORI

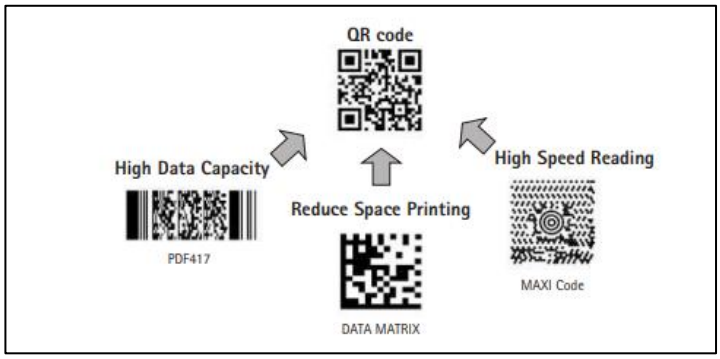
2.1 Tiket

Tiket adalah bukti legal yang diberikan kepada seseorang sebagai hak untuk mendapatkan layanan, memasuki suatu lokasi, atau menghadiri sebuah acara. Pada pelaksanaan suatu kegiatan, tiket berperan penting sebagai sarana pengendalian akses hanya individu yang berhak saja yang dapat masuk. Selain itu, tiket juga memiliki fungsi sebagai tanda pembayaran, pengatur jumlah peserta, serta media identifikasi bagi pemilik hak akses. Pada awalnya, tiket umumnya berbentuk fisik berupa karcis kertas yang mudah rusak dan rentan dipalsukan. Seiring perkembangan teknologi, tiket mulai bertransformasi menjadi tiket elektronik (e-ticket) yang lebih praktis (Margaretha & Voutama, 2023). *E-ticket* dapat disimpan dalam perangkat digital dan biasanya dilengkapi kode unik untuk memudahkan proses validasi. Salah satu bentuk inovasi e-ticket yang banyak digunakan saat ini adalah tiket berbasis *QR Code*, yang memungkinkan penyimpanan data lebih kompleks serta dapat diverifikasi secara cepat melalui perangkat pemindai digital. Perkembangan ini menunjukkan bahwa tiket tidak hanya berfungsi sebagai tanda masuk, tetapi juga sebagai instrumen penting dalam mendukung keamanan, kelancaran operasional, serta pengalaman pengguna dalam suatu acara.

2.2 Teknologi Pemindaian *QR CODE*

QR CODE adalah standar kode *QR* yang dikembangkan untuk memfasilitasi pembayaran digital di Indonesia. Teknologi ini memungkinkan pemindaian cepat dan akurat yang dapat digunakan untuk berbagai keperluan, termasuk verifikasi keaslian tiket (Eka Judistira et al, 2025). *QR CODE* dirancang untuk dapat digunakan oleh berbagai aplikasi dan sistem pembayaran, dengan penerapan yang luas di sektor publik maupun swasta (Mantik, 2021). *QR CODE* yang umumnya dikenal sebagai standar untuk pembayaran digital diadaptasi dalam penelitian ini untuk memverifikasi keaslian tiket secara cepat dan aman. Dalam aplikasi ini, *QR CODE* berfungsi sebagai alat untuk memastikan bahwa tiket yang dipindai memiliki informasi yang valid melalui pemindaian unik. *QR CODE* telah

berhasil diimplementasikan di berbagai sistem pembayaran digital di Indonesia, menunjukkan kecepatan dan fleksibilitasnya, yang menjadikannya pilihan yang tepat untuk verifikasi tiket secara *real-time* (Zalma Niendya Pangestika1, 2025).



Gambar 2.1 Pengembangan Kode *QR*

Sumber : (Zalma Niendya Pangestika, 2025)

Dalam penelitian ini, *QR CODE* digunakan untuk memverifikasi tiket pertandingan sepak bola melalui *platform mobile Android*. Keunggulan *QR CODE* dalam proses verifikasi adalah kemampuannya untuk di integrasi kan dengan *Algoritma Vigenere Cipher*, yang memastikan bahwa informasi dalam *QR CODE* tidak dapat dimodifikasi atau dipalsukan.

QR CODE dipilih karena keunggulannya dalam kecepatan pemindaian dan fleksibilitasnya untuk diintegrasikan dengan berbagai sistem (Faeruz Wafi Abidin et al, 2025). *QR CODE* mampu memverifikasi informasi secara cepat dan akurat, sehingga cocok digunakan dalam verifikasi tiket yang membutuhkan kecepatan dan keakuratan tinggi (Fatma Hairani, 2024), terutama pada event yang melibatkan banyak penonton seperti pertandingan sepak bola.

2.3 Android

Android adalah sistem operasi berbasis Linux yang dirancang khusus untuk perangkat bergerak seperti smartphone dan tablet. Sistem ini pertama kali dikembangkan oleh Android Inc sebelum diakuisisi oleh *Google* pada tahun 2005. Android bersifat terbuka (open source), sehingga memberi kebebasan bagi pengembang untuk melakukan modifikasi dan mengembangkan aplikasi sesuai kebutuhan. Keunggulan Android terletak pada fleksibilitas, dukungan komunitas pengembang yang luas, serta ketersediaan berbagai pustaka dan framework yang

mendukung pembuatan aplikasi (Tewari Singh, 2021). Selain itu, Android menyediakan Google Play Store sebagai sarana distribusi aplikasi, sehingga memudahkan pengguna dalam mengunduh dan memperbarui aplikasi. Dalam penelitian ini, Android dipilih karena merupakan sistem operasi yang paling banyak digunakan di Indonesia, sehingga memungkinkan aplikasi verifikasi tiket menjangkau lebih banyak pengguna. Android Studio sebagai *Integrated Development Environment* (IDE) resmi dari Google juga memberikan dukungan penuh untuk pengembangan aplikasi, mulai dari fitur debugging, emulator, hingga integrasi dengan pustaka eksternal untuk pemindaian *QR Code* dan pengolahan data secara *real-time*. Oleh karena itu, Android menjadi *platform* yang tepat untuk membangun aplikasi verifikasi tiket yang aman, efisien, dan mudah digunakan.

2.4 Aplikasi Android Studio

Android Studio adalah *Integrated Development Environment* (IDE) yang didesain untuk mengembangkan aplikasi *Android* (Siregar et al, 2023). *Android Studio* menyediakan berbagai alat yang memudahkan pengembang dalam membangun aplikasi *mobile*, termasuk pengujian, debugging, dan integrasi dengan berbagai pustaka eksternal seperti *ZXing Library* untuk pemindaian kode *QR* (Jurnal et al., 2022).

Penggunaan *Android Studio* dalam penelitian ini adalah untuk mengembangkan aplikasi yang mampu melakukan pemindaian tiket menggunakan kamera perangkat *mobile* dan memverifikasi data secara *real-time* melalui integrasi dengan *Firebase Realtime Database*. Fleksibilitas *Android Studio* memungkinkan pengembangan aplikasi yang mendukung berbagai fitur, seperti penggunaan *API,* pengolahan gambar, dan pengelolaan data yang diperlukan dalam sistem verifikasi tiket (Sondha et al., 2020). *Android Studio* adalah alat yang ideal untuk pengembangan aplikasi yang memerlukan interaksi langsung dengan perangkat keras seperti kamera, yang merupakan inti dari aplikasi ini.

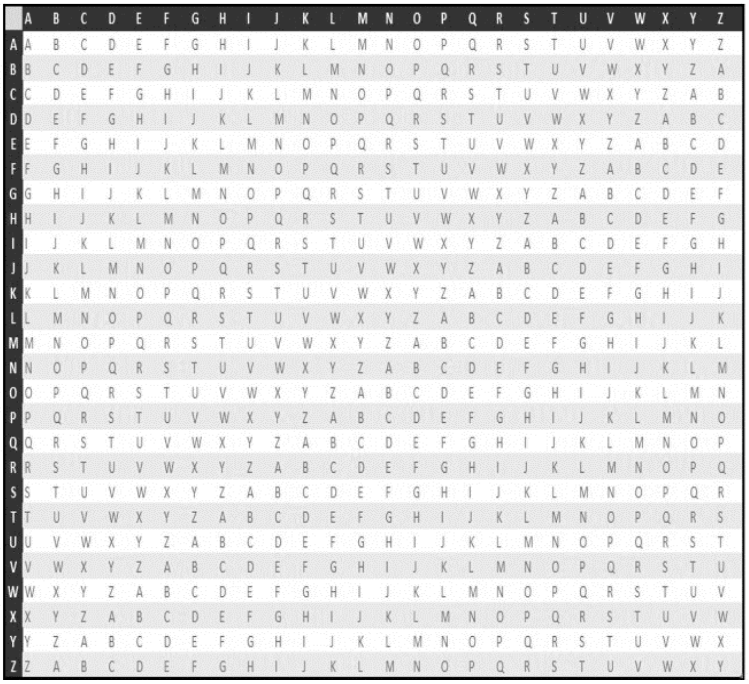
2.5 *Algoritma Vigenere Cipher*

Algoritma Vigenere Cipher merupakan salah satu *algoritma kriptografi* simetris *Vignere Cipher* dipilih dalam penelitian ini karena sifatnya yang menggunakan teknik substitusi polialfabetik lebih sederhana dan cocok untuk

meng*enkripsi* sistem dengan kebutuhan keamanan menengah (Alawiyah et al., 2020). Dibandingkan dengan *algoritma* modern seperti *AES* (*Advanced Encryption Standard*) atau *RSA* (*Rivest-Shamir-Adleman*), *Vigenere Cipher* memiliki kelebihan dari sisi implementasi yang lebih mudah serta penggunaan sumber daya yang lebih sedikit (Qowi, 2021). Walaupun *AES* dan *RSA* menawarkan tingkat keamanan lebih tinggi, kompleksitas serta kebutuhan komputasi tinggi mereka menjadikannya tidak ideal untuk aplikasi verifikasi tiket di level lokal seperti Persikotas Tasikmalaya. Selain itu, karena data yang diamankan bersifat terbatas (hanya data tiket dan tidak ada transaksi keuangan), *Vigenere Cipher* dipandang cukup efektif untuk keperluan ini. *Algoritma* ini bekerja dengan cara menggeser huruf-huruf pada pesan asli (*plaintext*) berdasarkan huruf pada kunci yang berulang, sehingga menghasilkan pesan terenkripsi (*ciphertext*) (Hammad et al., 2022). *Vigenere Cipher* memanfaatkan pola pengulangan kunci yang membuat setiap huruf dalam pesan terenkripsi memiliki pergeseran yang berbeda tergantung pada huruf kunci yang digunakan (Purwanti et al., 2024).

Proses *Enkripsi Vigenere Cipher* dimulai dengan memilih sebuah kunci yang terdiri dari serangkaian huruf, misalnya kunci "TIKET". Setiap huruf pada kunci kemudian dipasangkan dengan huruf-huruf pada pesan asli dan digeser sesuai dengan posisi abjad huruf kunci. Hasil pergeseran tersebut adalah teks terenkripsi yang tidak dapat dibaca tanpa mengetahui kunci yang digunakan. Langkah-langkah utama dalam *Algoritma Vigenere Cipher* adalah sebagai berikut:

1. Pemilihan Kunci: Pengguna memilih sebuah kunci (*key*) yang terdiri dari huruf-huruf. Kunci ini kemudian diulang sepanjang pesan asli.
2. Enkripsi: Setiap huruf dalam pesan asli digeser sesuai dengan posisi huruf yang sesuai dalam kunci. Proses ini menghasilkan teks terenkripsi yang sulit diuraikan tanpa kunci yang benar.
3. Deskripsi: Untuk mengembalikan pesan asli, pihak yang memiliki kunci dapat melakukan proses dekripsi dengan menggeser huruf dalam teks terenkripsi ke arah yang berlawanan, menggunakan kunci yang sama

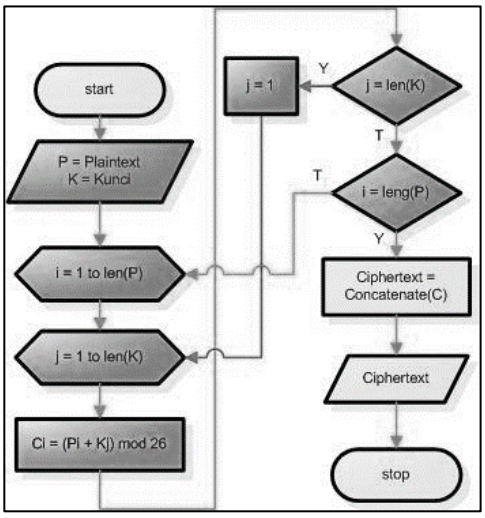


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 2.2 Pemetaan *Vigenere Cipher*

Sumber: (Ardhianto et al., 2021)

Gambar 2.2 menunjukkan *Vigenère Square* atau *Tabel Vigenère*, yaitu tabel yang digunakan dalam proses enkripsi dan dekripsi pada *Algoritma Vigenère Cipher*. Tabel ini terdiri dari baris dan kolom huruf alfabet A sampai Z. Baris pertama merepresentasikan huruf-huruf dari *plaintext* (teks asli), sedangkan kolom pertama menunjukkan huruf dari kunci (*key*). Proses *enkripsi* dilakukan dengan mencari titik temu antara huruf pada baris kunci dan huruf pada kolom *plaintext* untuk menghasilkan karakter sandi (*ciphertext*). Sebaliknya, proses dekripsi dilakukan dengan mencocokkan huruf *ciphertext* pada baris kunci dan menelusuri kolom yang sesuai untuk menemukan huruf *plaintext* aslinya.



Gambar 2.3 Alur Proses *Enkripsi Vigenere Cipher*

Sumber: (Ardhianto et al., 2021)

Gambar ini menggambarkan alur proses enkripsi *menggunakan Algoritma Vigenère Cipher*. Proses diawali dengan mendefinisikan *plaintext* (P) dan kunci (K). Selanjutnya, dilakukan perulangan untuk mencocokkan panjang kunci dengan panjang *plaintext*. Setiap karakter pada *plaintext* dan kunci dikonversi ke nilai numerik berdasarkan posisinya dalam alfabet (A = 0, B = 1, ..., Z = 25), kemudian dilakukan proses perhitungan dengan rumus (Pi + Ki) mod 26 untuk menghasilkan karakter sandi (*ciphertext*). Hasil enkripsi dari setiap karakter digabungkan untuk membentuk *ciphertext* akhir, lalu proses diakhiri.

Keunggulan *Algoritma Vigenere Cipher* dibandingkan dengan algoritma substitusi sederhana adalah tingkat keamanannya yang lebih tinggi karena penggunaan kunci yang berulang. Hal ini membuat pola pergeseran huruf lebih sulit ditebak dan mencegah analisis frekuensi pada pesan terenkripsi. Algoritma kriptografi modern seperti *AES* dan *RSA* menawarkan keamanan yang lebih tinggi, terutama untuk data sensitif seperti transaksi keuangan. Namun, dalam konteks verifikasi tiket, *Vigenere Cipher* memberikan keseimbangan yang baik antara keamanan dan efisiensi sumber daya (Alabady et al., 2025). Dengan data yang relatif sederhana, *Vigenere Cipher* mampu memberikan perlindungan yang memadai dengan komputasi yang lebih rendah dibandingkan algoritma modern,

sehingga lebih cocok untuk aplikasi berbasis android yang digunakan dalam verifikasi tiket.

Vigenere Cipher dipilih karena tingkat keamanannya yang memadai untuk aplikasi verifikasi tiket dan efisiensi sumber daya yang rendah, dibandingkan dengan *algoritma* modern seperti *AES* atau *RSA* yang biasanya digunakan dalam transaksi keuangan (Hidayah et al., 2023). Dalam konteks verifikasi tiket, *Vigenere Cipher* menyediakan perlindungan yang cukup tanpa memerlukan komputasi yang tinggi, menjadikannya solusi ideal untuk klub sepak bola lokal yang memiliki keterbatasan anggaran.

Meskipun *AES* dan *RSA* menawarkan keamanan yang lebih tinggi, penggunaan *Vigenere Cipher* dalam konteks ini lebih efisien dari sisi penggunaan sumber daya. Karena data yang dienkripsi adalah informasi tiket yang relatif sederhana dan bukan data finansial, *Vigenere Cipher* menawarkan perlindungan yang cukup memadai dengan kebutuhan komputasi yang lebih rendah, menjadikannya ideal untuk aplikasi verifikasi tiket pada klub lokal seperti Persikotas Tasikmalaya. *Algoritma Vigenere Cipher* juga telah digunakan dalam aplikasi pengamanan data di berbagai *platform* yang memerlukan keamanan tingkat menengah, seperti sistem verifikasi akses atau pengamanan komunikasi, yang menjadikannya ideal untuk konteks verifikasi tiket (Irianti et al., 2023).

2.6 *Firebase Realtime Database*

Firebase Realtime Database adalah solusi database berbasis *cloud* yang memungkinkan data disimpan dan disinkronkan secara *real-time* di semua klien. Dalam penelitian ini, *Firebase* digunakan untuk menyimpan dan memvalidasi data tiket yang telah terjual. Setiap kali petugas verifikasi memindai kode *QR* tiket, data tersebut dikirim ke *Firebase* untuk diverifikasi (Andrianto & Haris Munandar, 2022).

Firebase dipilih karena keunggulannya dalam menyediakan sinkronisasi data *real-time*, yang memastikan bahwa tiket yang dipindai oleh petugas akan divalidasi secara langsung di basis data. Hal ini sangat penting untuk menghindari tiket palsu atau tiket yang sudah pernah digunakan sebelumnya. *Firebase Realtime Database* dipilih karena kemampuannya dalam sinkronisasi data secara *real-time*

yang sangat dibutuhkan dalam proses verifikasi tiket (Imbalo Zaki Hasibuan & Triase, 2022). Selain itu, *Firebase* menawarkan integrasi yang lebih mudah dengan aplikasi *Android*, dibandingkan dengan *database* lain seperti *MongoDB* atau *PostgreSQL* yang mungkin memerlukan pengaturan lebih kompleks. *Firebase* juga mendukung pengelolaan data secara dinamis dengan keamanan yang diatur melalui *Firebase Authentication*, menjadikannya solusi ideal untuk pengembangan aplikasi *mobile* seperti ini.

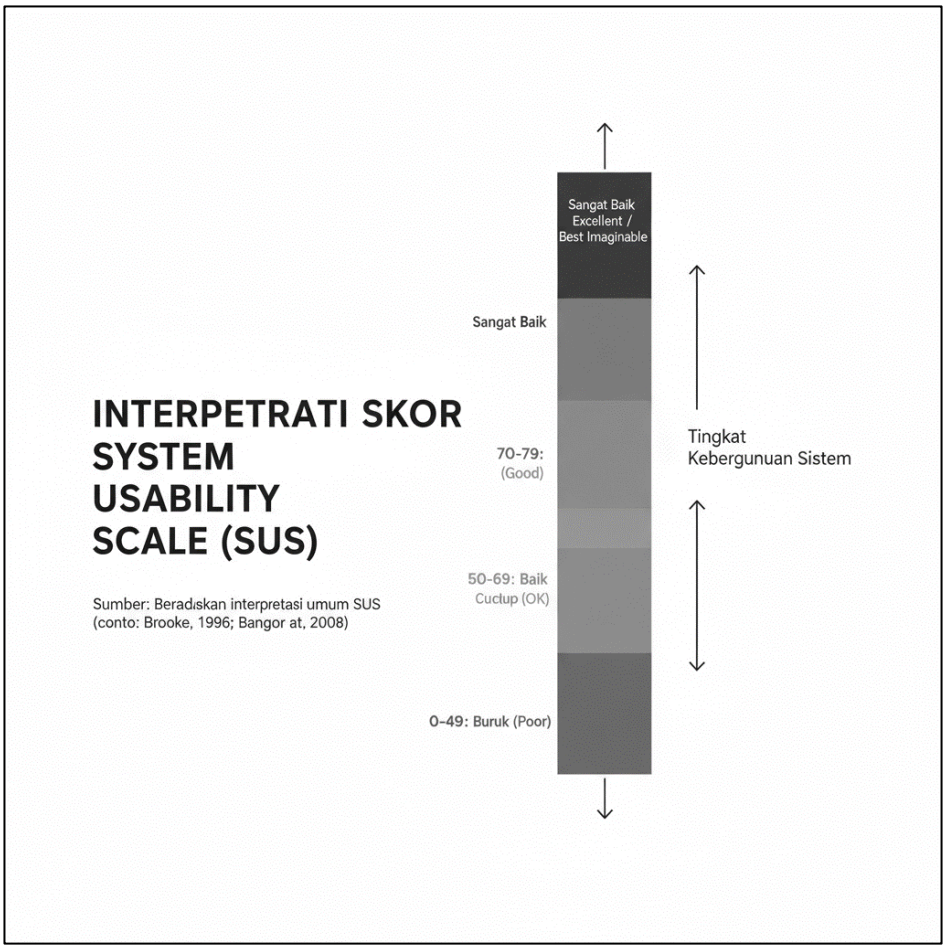
2.7 *Figma*

Figma adalah aplikasi desain berbasis web yang digunakan untuk membuat prototipe antarmuka pengguna (*UI*) dan pengalaman pengguna (*UX*). Aplikasi ini memungkinkan kolaborasi tim secara *real-time*, di mana desainer dan pengembang dapat bekerja bersama dalam satu proyek dari perangkat apapun (Al-Faruq et al., 2022). *Figma* mendukung pembuatan desain yang responsif, pengelolaan komponen *UI*, dan alur kerja yang terorganisir dengan baik. Dengan berbagai fitur seperti grid, pengeditan vektor, dan *prototyping* interaktif, *Figma* menjadi pilihan utama untuk mengembangkan aplikasi dan situs web yang *user-friendly* dan dinamis (Agus Muhyidin et al., 2020).

Dalam proyek ini, *Figma* digunakan untuk membuat prototipe antarmuka pengguna, mulai dari desain awal hingga pengujian interaktif. Misalnya, fitur seperti tombol pemindaian *QR CODE* dan notifikasi hasil verifikasi dirancang dengan menggunakan prototyping interaktif, memungkinkan petugas verifikasi untuk mencoba alur aplikasi secara *virtual* sebelum pengembangan final dilakukan.

2.8 Uji Validitas dengan *System Usability Scale* (SUS)

SUS adalah alat ukur sederhana namun efektif yang digunakan untuk mengevaluasi tingkat kegunaan (*usability*) dari sebuah aplikasi atau sistem (Galuh Sembodo et al., 2021).



Gambar 2.3 Interpolasi Skor SUS

(Galuh Sembodo et al., 2021)

Dalam konteks penelitian ini, *SUS* digunakan untuk mengukur kemudahan penggunaan aplikasi verifikasi tiket berbasis *Android* yang menggunakan pemindaian kode *QR* dan *enkripsi Vigenere Cipher*. *SUS* memiliki beberapa kelebihan yang menjadikannya metode yang populer di berbagai penelitian:

1. *SUS* relatif cepat dan mudah diterapkan karena terdiri dari 10 pertanyaan sederhana.
2. *SUS* bersifat agnostik terhadap teknologi, sehingga dapat diterapkan pada berbagai jenis aplikasi dan antarmuka pengguna (*user interface*).
3. Kuesioner *SUS* menghasilkan skor dalam rentang 1 – 100, yang memudahkan dalam evaluasi baik secara individu maupun kelompok.

Setiap pertanyaan dalam *SUS* menggunakan skala likert lima poin, mulai dari "Sangat Tidak Setuju" hingga "Sangat Setuju." Pertanyaan ini mencakup aspek-aspek seperti kenyamanan navigasi, kemudahan dalam penggunaan fitur, serta keseluruhan pengalaman pengguna. Skor *SUS* diperoleh dengan menggabungkan skor setiap pertanyaan, yang kemudian diinterpretasikan dalam bentuk persentase atau kelas huruf (*letter grades*) dari A hingga F (Alvian Kosim et al., 2022). Prosedur perhitungan skor SUS dilakukan sebagai berikut:

1. Untuk pernyataan ganjil (positif):
   Skor = Nilai jawaban – 1
2. Untuk pernyataan genap (negatif):
   Skor = 5 – Nilai jawaban

Selanjutnya, seluruh skor dari 10 pernyataan dijumlahkan, lalu hasilnya dikalikan dengan 2,5 untuk mendapatkan skor akhir *SUS* dalam rentang 0 sampai 100. Skor ini tidak mewakili persentase, melainkan sebagai ukuran relatif tingkat kegunaan sebuah sistem.

SUS dipilih dalam penelitian ini karena kesederhanaannya, namun tetap efektif dalam menghasilkan wawasan yang jelas tentang tingkat kegunaan aplikasi. Ini sangat penting untuk mengetahui apakah aplikasi verifikasi tiket ini sudah user-friendly dan memenuhi kebutuhan pengguna secara optimal.

Interpretasi Skor *SUS* nilai *SUS* yang diperoleh kemudian diinterpretasikan ke dalam kelas huruf sebagai berikut:

- Grade A: nilai >= 80.3
- Grade B: nilai 74 – <80.3
- Grade C: nilai 68 – <74
- Grade D: nilai 51 – <68
- Grade F: nilai < 51

Dalam penelitian ini, nilai *SUS* yang dihasilkan akan digunakan untuk mengevaluasi tingkat kegunaan aplikasi verifikasi tiket secara keseluruhan, serta memberikan umpan balik yang bermanfaat untuk perbaikan lebih lanjut.

2.9 Penelitian Terkait *(State of the Art)*

Berbagai penelitian telah dilakukan sebelumnya yang terkait dengan pengembangan sistem verifikasi tiket dan penggunaan *QR CODE*. Dalam tabel berikut, beberapa penelitian penting yang mendasari pengembangan aplikasi ini dirangkum:

Tabel 2.1 State Of The Art

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
1.	Rancang Bangun Sistem Ketertelusuran Kakao Berbasis Aplikasi Web dan *QR CODE Building Cocoa Traceab*	Ismail Sulaiman, Yusriana, Wawan Muliawan, 2021	*System Development Life Cycle* (SDLC)	Hasil penelitian menunjukkan bahwa sistem ketertelusuran kakao berhasil dikembangkan dalam bentuk aplikasi web dan *QR CODE,* yang memungkinkan informasi dapat diakses melalui internet dan aplikasi memindai *QR* di ponsel. Sistem ini melibatkan 7 admin dan mencakup proses input, output, penyimpanan, dan kontrol untuk memastikan ketertelusuran kakao yang efektif.
2.	Modifikasi *Algoritma Vigenere Cipher* dengan Pembangkit Kunci Random Number Generator Dalam Pengamanan Citra Digital	Shafira Amalia Zebua, 2022	*Vigenère Cipher*	Hasil penelitian menunjukkan bahwa penggabungan *Vigenere Cipher* dengan *RNG-LCG* meningkatkan keamanan citra digital, membuatnya lebih sulit untuk dimanipulasi atau disalahgunakan oleh pihak yang tidak berwenang.
3.	*Algoritma Caesar Cipher atau Vigenere Cipher* pada	Vara Maulidyah Hidayah, Dadang Iskandar Mulyana,	*Caesar Cipher* dan *Vigenere Cipher*	Hasil penelitian menunjukkan bahwa kombinasi algoritma *Caesar Cipher* dan *Vigenere Cipher* dapat digunakan untuk

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
	Pengenkripsian Pesan Teks	Yuliana Bachtiar, 2023		menghasilkan pesan teks rahasia. Proses enkripsi dan dekripsi berhasil dilakukan, dan teks asli dapat diubah menjadi *ciphertext* serta dikembalikan menjadi *plaintext*. Penelitian ini juga mencatat bahwa penggunaan kunci acak meningkatkan keamanan penginputan teks
4.	Teknik Keamanan Data Menggunakan Metode *Vigenere Cipher* Dan *Steganografi* Dalam Penyisipan Pesan Teks Pada Citra	Rahmad Prayogi Harahap, Abdul Halim Hasugian, 2023	Penelitian ini menggunakan *Vigenere Cipher* untuk enkripsi pesan teks dan *steganografi* untuk menyisipkan pesan teks ke dalam citra.	Penggunaan kedua metode ini secara bersamaan terbukti meningkatkan keamanan data dalam pertukaran pesan teks. Pesan tidak hanya terenkripsi tetapi juga tersembunyi secara visual dalam citra, membuatnya lebih sulit diakses oleh pihak yang tidak berwenang. Penelitian ini juga mengidentifikasi tantangan seperti ukuran citra, kualitas citra, dan proses dekripsi.
5.	Peningkatan Keamanan Data Melalui Teknik Super Enkripsi Menggunakan *Algoritma Vigenere dan Caesar*	Eko Nur Wahyudi, Eka Ardhianto, Widiyanto Tri Handoko, Hari Murti, Edy Supriyanto, Endang	*Cesar Cipher* Standard dan *Vigenere Autokey*	Hasil penelitian menunjukkan bahwa nilai entropi dari metode super enkripsi adalah 4,972, yang lebih baik dibandingkan dengan nilai entropi sebelumnya yaitu 4,689. Peningkatan ini menunjukkan tingkat keamanan data meningkat dari

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
		Lestariningsih, Rara Sriartati Redjeki, 2024		58,62% menjadi 62,15%. Ukuran file *cipherteks* dan *plainteks* tidak mengalami perubahan, sehingga tidak memerlukan lebih banyak sumber daya penyimpanan. Ukuran file optimal untuk enkripsi adalah 16 kilobyte dengan nilai entropi tertinggi mencapai 5,095.
6.	Implementasi Kriptografi pada Pengamanan Data Pembayaran Piutang Pelanggan Menggunakan *Vigenere Cipher*	Risna, Yusni Amaliah, Selly Yunita, 2022	kriptografi simetri dengan *Algoritma Vigenere Cipher*	Hasil penelitian menunjukkan bahwa *Algoritma Vigenere Cipher* berhasil digunakan untuk mengamankan data pembayaran pelanggan berupa file Excel. Proses enkripsi mengubah dokumen menjadi karakter yang sulit dimengerti dan hanya dapat didekripsi dengan kunci yang sama. Pengujian *blackbox* membuktikan bahwa sistem berjalan sesuai dengan harapan dan mampu menjaga data dari manipulasi pihak yang tidak berwenang.
7.	Analisis Keamanan Data Pelanggan Menggunakan *Algoritma Vigenere*	Erika Tangsi Rante, Muhammad Alnando, Mistu Heru, Kevin Junior, 2023	*Algoritma Vigenere Cipher* dan *Playfair Cipher*	Kombinasi metode enkripsi dengan *Algoritma Vigenere Cipher* dan Playfair Cipher menghasilkan ciphertext yang lebih sulit untuk dipecahkan, bahkan

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
	Cipher dan *Playfair Cipher*			menggunakan metode serangan klasik. Hal ini membuat analisis frekuensi menjadi sangat rumit karena karakter dalam *ciphertext* lebih seragam. Kombinasi kedua algoritma ini terbukti efektif untuk mengamankan data pelanggan dari risiko akses tidak sah dan pelanggaran keamanan.
8.	*Teknik Algoritma Vigenere Chiper* dalam *Steganografi* dalam Keamanan Sistem Komputer	Rachmat Destriana, 2022	*Vigenere Cipher*	Hasil penelitian menunjukkan bahwa teknik *Algoritma Vigenere Cipher* dapat diimplementasikan dengan baik dalam steganografi dan mampu menyembunyikan rahasia pesan dalam file gambar tanpa terlihat perbedaan yang signifikan antara file gambar asli dan file gambar yang telah dimodifikasi.
9.	Implementasi kombinasi algoritma *myszkowski transposition* dan *vigenere cipher* pada keamanan untuk file teks	Meylissa, Khairil, Juju Jumadi, 2023	Penelitian ini menggabungkan *Myszkowski Transposition* dan *Vigenere Cipher* untuk meningkatkan keamanan data.	Hasil analisis dan pengujian menunjukkan bahwa tanpa kunci yang sesuai, *ciphertext* tidak dapat dikembalikan ke *plaintext*, yang membuktikan bahwa metode ini memiliki tingkat keamanan yang lebih baik dibandingkan jika kedua algoritma digunakan secara terpisah. Sistem ini

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
				menggunakan kriptografi simetris, sehingga dekripsi hanya bisa dilakukan dengan kunci yang sama seperti saat enkripsi.
10.	Implementasi kriptografi kombinasi *Algoritma Vigenere Cipher* dan *reverse cipher* untuk keamanan teks pada aplikasi catatan pribadi berbasis android	MF Siregar, 2024	*Vigenere Cipher* dan *Reverse Cipher*	Hasil dari penelitian menunjukkan bahwa implementasi kriptografi dalam aplikasi ini berhasil meningkatkan keamanan data pribadi. Aplikasi yang dirancang dapat melakukan enkripsi dan dekripsi pesan dengan baik, sehingga memastikan kerahasiaan data pengguna. Selain itu, aplikasi ini memberikan fitur yang membedakannya dari aplikasi catatan pribadi lainnya yang tidak memiliki fitur kriptografi
11.	Penerapan Algoritma *AES* pada *QR CODE* untuk Keamanan Verifikasi Tiket	Adiat Pariddudin dan Fatih Syauqi ,2020	*AES*	Penelitian ini berhasil menerapkan algoritma *AES* (Advanced Encryption Standard) pada *QR CODE* untuk meningkatkan keamanan sistem verifikasi tiket. Hasilnya menunjukkan bahwa enkripsi *AES* mampu mengamankan data tiket dari duplikasi atau manipulasi, sehingga hanya tiket asli yang dapat diverifikasi. Sistem yang dikembangkan memungkinkan *QR CODE* tiket berubah

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
				setiap 60 detik, sehingga memperkecil kemungkinan penyalahgunaan. Dengan teknologi ini, proses verifikasi tiket menjadi lebih cepat, efisien, dan aman, memberikan perlindungan lebih bagi penyelenggara acara maupun pengguna tiket.
12.	Evaluasi *Usability* Website Shopee Menggunakan *System Usability Scale* (*SUS*)	Firman Galuh Sembodo, Gita Fadila Fitriana, Novian Adi Prasetyo, 2021	*System Usability Scale* (*SUS*)	Rata-rata skor *SUS* yang diperoleh adalah 67,08, yang menurut interpretasi masuk dalam kategori "OK/Fair". Uji T-Test menghasilkan nilai signifikansi 0,716 (lebih dari 0,05), sehingga hipotesis nol diterima. Artinya, tidak terdapat perbedaan signifikan antara skor usability Shopee dan nilai referensi *SUS* (68). Secara keseluruhan, website Shopee dinilai cukup layak digunakan dari sisi usability, meskipun masih terdapat ruang perbaikan.
13.	Implementasi Kriptografi *Vigenere Cipher* untuk Keamanan Data Informasi Desa	Erva Irianti, Dewi Fatmarani Surianto, Ainun Zahra Adistia, Muh. Juharman, Jumadil Ahmad Safi'i, 2023	*Vignere Cipher*	Aplikasi berhasil mengenkripsi dan mendekripsi data penting seperti daftar penerima bantuan di desa (PKH, BPNT, KIP, BLT). Dengan menambahkan kunci enkripsi, data *plaintext* diubah menjadi *ciphertext* melalui pergeseran karakter berbasis alfabet. Proses ini meningkatkan keamanan karena data tidak dapat dibaca

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
				atau diubah oleh pihak yang tidak berwenang. Aplikasi diuji melalui simulasi dan menunjukkan bahwa informasi desa dapat diamankan dengan baik menggunakan teknik *Vigenère Cipher*.
14.	*Algoritma Caesar Cipher* atau *Vigenere Cipher* pada Pengenkripsian Pesan Teks	Vara Maulidyah Hidayah, Dadang Iskandar Mulyana, Yuliana Bachtiar, 2023	*Caesar Cipher* dan *Vigenère Cipher*	Aplikasi yang dikembangkan mampu menyandikan pesan (plaintext) menjadi *ciphertext* dan mengembalikannya lagi ke *plaintext* menggunakan kunci (key) tertentu. Implementasi kombinasi *algoritma Caesar* dan *Vigenère* terbukti mampu meningkatkan keamanan teks dengan membuat hasil enkripsi sulit ditebak, bahkan jika pesan awal sama namun menggunakan kunci yang berbeda. Penelitian juga menyimpulkan bahwa metode ini cocok untuk pengamanan data berskala ringan hingga menengah, seperti penginputan data teks, dengan efisiensi tinggi dan sumber daya minim.
15.	*Enhanced Vigenere Cipher Algorithm for Improved Cryptographic Security*	S.A. Alabady, T.F. Shawkat, A.W. Adrees, 2024	*Enhanced Vigenère Cipher*	Algoritma yang diperbarui menunjukkan peningkatan signifikan dalam ketahanan terhadap analisis frekuensi dan serangan Kasiski. Metode ini berhasil menyembunyikan pola kunci berulang yang menjadi kelemahan utama *Vigenère*

No	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
				klasik. Hasil pengujian juga menunjukkan kinerja efisien pada perangkat dengan keterbatasan sumber daya karena ringan secara komputasi. Pendekatan ini memperbesar ruang kunci (keyspace)meningkatkan difusi serta konfusi *ciphertext*, sehingga menyulitkan serangan *brute-force*. Meski demikian, studi ini juga mencatat bahwa manajemen kunci tetap menjadi tantangan dalam implementasi skala besar.

Tabel 2.2 Matriks Penelitian

No.	Penulis	Ruang Lingkup													
		Metode				*Platform*		*Algoritma*						Pengujian	
		MDLC	**SDLC**	**R&D**	***Waterfall***	***ndroid***	***Web***	***Vigenere Cipher***	***RSA***	***Caesar Cipher***	***Reverse Cipher***	***AES***	Reverse Cipher	***Black Box***	**SUS**
1.	(Ismail Sulaiman, Yusriana, Wawan Muliawan, 2021)		✓				✓							✓	
2.	(Shafira Amalia Zebua, 2022)	✓					✓	✓							
3.	(Vara Maulidyah Hidayah, Dadang Iskandar Mulyana, Yuliana Bachtiar, 2023)				✓		✓	✓		✓					
4.	(Rahmad Prayogi Harahap, Abdul Halim Hasugian, 2023)	✓					✓	✓						✓	

5.	(Eko Nur Wahyudi, Eka Ardhianto, Widiyanto Tri Handoko, Hari Murti, Edy Supriyanto, Endang Lestariningsih, Rara Sriartati Redjeki, 2024)			✓		✓		✓							
6.	(Risna, Yusni Amaliah, Selly Yunita, 2022)		✓				✓	✓						✓	
7.	(Erika Tangsi Rante, Muhammad Alnando, Mistu Heru, Kevin Junior, 2023)					✓		✓						✓	
8.	(Rachmat Destriana, 2022)							✓					✓		
9.	(Meylissa, Khairil, Juju Jumadi, 2023)							✓					✓		
10.	(MF Siregar, 2024)	✓				✓		✓			✓		✓		
11.	(Adiat Pariddudin,Fatih Syauqi ,2020)		✓				✓					✓		✓	
12.	(Firman Galuh Sembodo, Gita Fadila Fitriana, Novian Adi Prasetyo , 2021)				✓		✓							✓	✓
13.	(Erva Irianti, Dewi Fatmarani Surianto, Ainun Zahra Adistia, Muh. Juharman, Jumadil Ahmad Safi'i, 2023)		✓			✓		✓							

14.	(Vara Maulidyah Hidayah, Dadang Iskandar Mulyana, Yuliana Bachtiar, 2023)			✓		✓		✓							
15.	(S.A. Alabady, T.F. Shawkat, A.W. Adrees, 2024)				✓			✓							

2.10 Relevansi Penelitian

Penelitian yang terdekat mengenai sistem *ticketing* dilakukan oleh Isti Rahayu et al (2024), berfokus pada pengembangan sistem penjualan tiket konser musik berbasis web dengan pemanfaatan barcode sebagai tanda pengenal unik pada setiap tiket. Sistem yang dirancang bertujuan untuk mengatasi permasalahan umum dalam penyelenggaraan konser, seperti antrean panjang di pintu masuk, gangguan pada proses transaksi, serta pengelolaan data pembeli yang kurang efisien. Melalui penerapan *barcode*, setiap tiket memiliki identitas yang berbeda sehingga dapat meminimalisir potensi duplikasi maupun pemalsuan tiket. Hasil penelitian menunjukkan bahwa penggunaan barcode mampu meningkatkan efisiensi distribusi tiket sekaligus mempercepat proses validasi di lapangan. Akan tetapi, penelitian tersebut belum mengintegrasikan aspek keamanan berbasis kriptografi, sehingga data yang tersimpan dalam barcode masih berpotensi diakses maupun dimanipulasi oleh pihak yang tidak bertanggung jawab.

Berdasarkan kelemahan tersebut, penelitian ini menawarkan pengembangan sistem ticketing untuk pertandingan sepak bola dengan mengganti penggunaan barcode konvensional menjadi *QR Code*. *QR Code* dipilih karena memiliki kapasitas penyimpanan lebih besar, fleksibilitas lebih tinggi, serta kompatibilitas yang luas dengan perangkat pemindai modern. Untuk menambah lapisan keamanan, data yang terkandung dalam *QR Code* dienkripsi menggunakan *Algoritma Vigenère Cipher*. Dengan cara ini, informasi tiket hanya dapat dibaca oleh pihak yang memiliki kunci dekripsi yang tepat, sehingga risiko pemalsuan dan manipulasi data dapat diminimalkan. Perbedaan mendasar ini menjadi kontribusi utama penelitian, yaitu menghadirkan sistem *ticketing* yang tidak hanya efisien, tetapi juga memiliki tingkat keamanan yang lebih baik dibanding penelitian sebelumnya.