BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Berikut ini merupakan penelitian-penelitian sejenis yang ditemukan peneliti dalam bentuk jurnal, antara lain:

2.1.1 Pengembangan Sistem Informasi Asosiasi Jasa Konstruksi dengan Menerapkan Tanda Tangan Digital

Abdurrachman dan Suteja (2021) melakukan penelitian yang mengembangkan sistem informasi untuk asosiasi jasa konstruksi yang terintegrasi dengan Sistem Informasi Konstruksi Indonesia (SIKI) LPJK. Dalam penelitian tersebut, tanda tangan digital diterapkan pada dokumen keanggotaan dengan memanfaatkan algoritma Advanced Encryption Standard (AES) dan Secure Hash Algorithm (SHA). Hasil penelitian mengungkapkan bahwa sistem ini berhasil meningkatkan keamanan dokumen dan mempercepat proses verifikasi melalui penggunaan QR Code.

2.1.2 Rancang Bangun Sistem Validasi Surat Akademik Menggunakan QR Code dan Algoritma AES pada Siakadbeta Universitas HaluOleo

Penelitian ini bertujuan untuk menciptakan sistem yang dapat memvalidasi surat akademik dengan memanfaatkan teknologi Kode QR dan algoritma Advanced Encryption Standard (AES). Sistem ini dirancang untuk menjamin keaslian dan integritas dokumen akademik di Universitas Halu Oleo, yang sebelumnya mengalami kesulitan dalam validasi karena masih mengandalkan metode tradisional. Algoritma AES diterapkan untuk mengenkripsi data dokumen, sementara QR Code digunakan untuk mempermudah proses validasi dokumen secara otomatis. Dari hasil pengujian menunjukkan bahwa sistem dapat berfungsi dengan efektif, meskipun kinerja validasi dipengaruhi oleh jumlah data yang tersimpan dalam QR Code dan kemampuan alat pemindai yang digunakan (Surimi et al., 2023).

2.1.3 Implementasi Algoritma HMAC-SHA-256 Untuk Keamanan Kemasan Produk

Penelitian yang dilakukan oleh Angkasa, Asriyanik, dan Pambudi (2023) bertujuan untuk meningkatkan keamanan produk yang menerapkan algoritma HMAC-SHA-256 sebagai alternatif kemamanan bagi segel kemasan produk. Algoritma ini menggabungkan fungsi hash dan kunci untuk menghasilkan Kode Autentikasi Pesan (MAC), yang kemudian diintegrasikan ke dalam kode QR. Dari hasil pengujian menunjukkan bahwa sistem ini berhasil meningkatkan keamanan produk melalui komputasi yang cepat dan efektif dalam mencegah pemalsuan kemasan dengan menggunakan segel keamanan berbasis QR Code.

2.1.4 Centralized Threshold Key Generation Protocol Based on Shamir Secret Sharing and HMAC Authentication

Penelitian ini bertujuan untuk mengembangkan protokol pembuatan kunci ambang terpusat yang efisien dengan menggunakan teknik berbagi rahasia Shamir dan mendukung otentikasi kunci menggunakan protokol Hashed Message Authentication Code (HMAC). Protokol ini memungkinkan manajer grup untuk membagi kunci rahasia utama menjadi beberapa bagian rahasia yang didistribusikan kepada anggota kelompok. Otentikasi kunci dilakukan menggunakan HMAC untuk memverifikasi identitas dan menjaga kerahasiaan kunci. Hasilnya, protokol yang diusulkan mampu mengurangi biaya komputasi dan komunikasi dengan tetap menjaga keamanan dan integritas kunci rahasia dalam jaringan (Abdel Hakeem & Kim, 2022).

2.1.5 Perancangan Sistem Tanda Tangan Digital (Digital Signature)

Tujuan penelitian ini adalah merancang sistem tanda tangan digital yang dapat mengidentifikasi pengirim serta memverifikasi keaslian dokumen digital yang dikirimkan melalui internet. Sistem ini memanfaatkan perangkat lunak EJBCA sebagai Server RootCA untuk digunakan

menghasilkan sertifikat digital untuk selanjutnya digunakan dalam proses penandatanganan dan verifikasi dokumen digital. Berdasarkan hasil penelitian, sistem ini berhasil menghasilkan sertifikat digital yang dapat digunakan untuk menandatangani berbagai jenis file, termasuk Doc, PDF, dan Email (Taufiqurrahman et al., 2020).

Tabel 2.1 Perbandingan Penelitian Terdahulu

Aspek	**Abdurrachman & Suteja (2021)**	**Surimi et al. (2023)**	**Angkasa et al. (2023)**	**Penelitian Ini**
Ruang Lingkup	Sektor jasa konstruksi	Surat akademik	Keamanan kemasan produk	Penandatanganan elektronik di perusahaan agribisnis
Manajemen Dokumen	Tidak ada	Tidak ada	Tidak ada	Terpusat
Metode Enkripsi	AES	AES	HMAC-SHA-256	AES-128 dan HMAC-SHA256
Media Penyimpanan	QR Code	QR Code	-	QR Code
Integritas Data	Tidak ada	Tidak ada	HMAC-SHA-256	HMAC-SHA256
Tujuan Utama	Keabsahan dokumen	Validasi surat akademik	Keamanan kemasan produk	Keamanan dan efisiensi penandatanganan dokumen
Fitur Notifikasi	Tidak ada	Tidak ada	Tidak ada	Ada

2.2 Teori Terkait

Teori yang relevan dalam penelitian ini mencakup konsep-konsep yang berkaitan erat dengan masalah yang diteliti, seperti sistem penandatanganan elektronik, QR Code, sertifikat digital, algoritma enkripsi AES-128, dan HMAC-SHA256. Teori-teori ini berperan sebagai dasar pemikiran dan argumen dalam menyelesaikan masalah penelitian. Berikut adalah uraian teoritis yang relevan:

2.2.1 Tanda Tangan Elektronik

Tanda Tangan Elektronik merupakan bentuk tanda tangan yang terdiri dari informasi elektronik yang terhubung atau berkaitan dengan informasi elektronik lain. Fungsi utamanya adalah sebagai alat untuk verifikasi dan autentikasi, yang memastikan asal, integritas, dan keutuhan informasi atau dokumen elektronik yang digunakan oleh organisasi atau lembaga komersial. Penanda Tangan adalah subjek hukum yang terhubung atau berkaitan dengan Tanda Tangan Elektronik (Kementerian Komunikasi dan Informatika Republik Indonesia, 2022).

Terdapat dua jenis aturan terkait tanda tangan elektronik, yaitu tanda tangan yang memiliki sertifikasi dan tidak memiliki sertifikasi. Tanda tangan yang memiliki sertifikasi menggunakan sistem sandi atau kriptografi yang diresmikan oleh BSSN (Badan Standardisasi dan Sertifikasi Nasional) melalui sertifikat digital. Tanda tangan ini memenuhi persyaratan sah sebagai tanda tangan digital sesuai dengan ketentuan undang-undang. Sementara itu, tanda tangan yang tidak memiliki sertifikasi menggunakan Kode QR sebagai elemen pendukung untuk memastikan keabsahan dokumen fisik ketika dicetak. Hal ini sejalan dengan Peraturan Pemerintah (PP) No. 82 Tahun 2012 yang telah diperbarui menjadi Peraturan Pemerintah (PP) No. 71 Tahun 2019 (Mubaroq & Fitria, 2021).

Meskipun QR code bukan tanda tangan elektronik tersertifikasi, QR code dapat menjadi bagian dari mekanisme yang memastikan keabsahan dan keamanan dokumen. Apalagi jika dipadukan dengan mekanisme kriptografi yang sesuai, QR code dapat memenuhi syarat sah sebagai tanda tangan elektronik.

Beberapa regulasi yang mengatur tentang tanda tangan elektronik dapat ditemukan pada halaman regulasi website Badan Penyelenggara Sertifikasi Elektronik (PSrE) yang berada di bawah Kementerian Kominfo (2024). Beberapa di antaranya adalah:

a. Peraturan Menteri Kominfo Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik
b. Peraturan Pemerintah PSTE Nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
c. Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2.2.2 Quick Response (QR) Code

QR Code, atau kode QR, merupakan pengembangan dari barcode. Jika barcode memiliki bentuk satu dimensi, kode QR memiliki bentuk dua dimensi. Dibandingkan dengan barcode, kode QR dapat menyimpan data yang lebih besar dengan membuat penandaan dua dimensi pada permukaannya (Indriyawati et al., 2021). Teknologi ini pertama kali dikembangkan oleh Denso Wave pada tahun 1994 dan dapat menyimpan berbagai jenis data berupa informasi, seperti huruf, angka, dan data lainnya, dengan kapasitas hingga 7.089 karakter. Sebagai perbandingan, barcode konvensional hanya dapat menyimpan sekitar 20 digit. Selain itu Kode QR memiliki ukuran cetak yang kecil, tahan terhadap kotoran dan kerusakan serta kemampuan membaca dari berbagai arah (Mohammed Ali & Farhan, 2020). Proses pengenalan pola pada kode QR melalui deteksi marker atau tanda yang terisi dengan informasi yang diperlukan. Tidak seperti barcode yang hanya mampu menyimpan data secara satu dimensi (horizontal), kode QR dapat menyimpan informasi secara dua dimensi, baik horizontal maupun vertikal. Hal ini memungkinkan kode QR untuk menampung lebih banyak informasi, seperti URL, teks, angka, dan lainnya (Alfatihah et al., 2021).

Kode QR telah digunakan untuk banyak tujuan seperti fitur keamanan atau metode verifikasi dokumen. Namun, verifikasi dengan hanya menggunakan kode QR memiliki kelemahan, seperti data yang dapat

dimanipulasi. Untuk mengatasi kelemahan kode QR, data yang disisipkan dalam kode QR harus dienkripsi (Indriyawati et al., 2021).

Dalam penelitian ini, QR Code digunakan sebagai media penyimpanan informasi penandatanganan yang telah dienkripsi menggunakan algoritma AES-128. Informasi ini meliputi nomor surat, ID pengguna, timestamp, dan HMAC dari tanda tangan sebelumnya (jika ada). QR Code kemudian disematkan pada dokumen PDF sebagai bagian dari tanda tangan digital.

2.2.3 Advanced Encryption Standard (AES)

AES adalah algoritma enkripsi yang diciptakan oleh dua ahli kriptografi, yaitu Dr. Vincent Rijmen dan Dr. Joan Daemen, yang berasal dari Belgia. Algoritma ini pertama kali dikembangkan pada tahun 1997. Selanjutnya, AES diajukan sebagai kandidat dan akhirnya pada November 2001 ditetapkan sebagai standar enkripsi oleh National Institute of Standards and Technology (NIST) (Alfatihah et al., 2021). AES kemudian diumumkan oleh NIST pada tahun 2001 sebagai algoritma enkripsi simetris (Marqas et al., 2020).

AES adalah algoritma kriptografi simetris, artinya kunci yang digunakan dalam proeses mengenkripsi dan mendekripsi adalah sama. Dengan demikian, dalam melakukan enkripsi dan dekripsi, AES mengandalkan satu kunci yang identik. Algoritma ini telah diadopsi secara luas sebagai standar enkripsi di banyak negara, termasuk Amerika Serikat. AES mendukung panjang kunci 128 bit (16 byte), 192 bit (24 byte), atau 256 bit (32 byte), dengan jumlah putaran enkripsi sebanyak 10 putaran. AES dikenal sebagai algoritma yang sangat kuat, dan hingga saat ini belum terdapat laporan serangan yang berhasil membobolnya melalui kriptanalisis (Zulfikar et al., 2023).

Pemilihan penggunaan AES karena memiliki beberapa keunggulan jika dibandingkan dengan RSA (Rivest Shamir Adleman). Dari segi waktu eksekusi, AES lebih cepat daripada RSA karena RSA memerlukan perhitungan yang lebih kompleks (Fajrin et al., 2024). Kinerja waktu AES dalam proses enkripsi dan dekripsi juga lebih baik dibandingkan RSA,

terutama ketika ukuran data yang dienkripsi semakin besar (Laurentinus et al., 2020). Hal ini juga ditunjukan pada hasil percobaan bahwa AES memiliki waktu eksekusi yang lebih baik dibandingkan RSA dalam enkripsi dan dekripsi (Marqas et al., 2020). Meskipun demikian, dari segi keamanan, AES dan RSA memiliki tingkat keamanan yang setara, dan keduanya memenuhi standar yang digunakan dalam industri (Fajrin et al., 2024).

Dalam penelitian ini, AES-128 digunakan untuk mengamankan informasi penandatanganan, seperti nomor surat, ID pengguna, timestamp, dan HMAC dari tanda tangan sebelumnya (jika ada). Informasi ini kemudian dienkripsi dan disimpan dalam QR Code.

2.2.4 Hash-based Message Authentication Code (HMAC)

HMAC adalah teknik otentikasi kriptografi yang memanfaatkan fungsi hash dan kunci rahasia. HMAC merupakan algoritma MAC berbasis fungsi hash satu-arah yang mengimplementasikan mekanisme yang menggunakan fungsi hash seperti MD5 ataupun SHA1 dalam menghasilkan nilai MAC. Namun menurut Anugrah, Ichsan, dan Kusyanti (2019), algoritma HMAC dengan MD5 dan SHA1 memiliki kekurangan, seperti mudah terkena serangan brute force dan collision attack. SHA2, yang merupakan pengembangan dari SHA1, telah ditetapkan sebagai standar oleh NIST pada tahun 2010. Pada tahun 2017, ditemukan kerentanan pada SHA1 yang mendorong pengguna untuk beralih ke SHA2 (Stallings, 2022).

Tingkat keamanan HMAC sangat sulit ditembus karena penyerang perlu mengetahui kombinasi teks dan kunci yang benar. Algoritma hash SHA256 menawarkan tingkat keamanan dan kompleksitas yang tinggi. Untuk membongkar nilai hash SHA256, diperlukan upaya hingga 2256 kali percobaan (Rahim et al., 2023).

HMAC dapat digunakan untuk memverifikasi otentikasi pesan. Penerima pesan harus menentukan apakah telah menerima MAC yang sama menggunakan kunci rahasia yang sama dan pesan dianggap asli jika output MAC cocok dengan MAC yang dikirim oleh pengirim (Suhaili et al., 2024). Hal ini juga disebutkan pada penelitian lain, dimana proses otentikasi dilakukan menggunakan protokol HMAC-SHA256 dengan membandingkan nilai hash

dari pesan yang diterima. Jika menghasilkan nilai hash yang sama maka dapat membuktikan kerahasiaan serta memastikan integritas dan otentikasi pesan selama transmisi (Abdel Hakeem & Kim, 2022).

Dengan menggunakan fungsi hash HMAC-SHA256 akan menghasilkan nilai MAC sebagai message digest yang pada penelitian ini akan disertakan dengan informasi penandatangan yang di tempatkan pada kode QR. Message digest ini akan digunakan sebagai validasi bahwa tidak ada perubahan pada informasi penandatanganan serta digunakan memverifikasi hirarki penandatanganan, di mana setiap tanda tangan terkait dengan tanda tangan sebelumnya.

2.2.5 Enterprise JavaBeans Certificate Authority (EJBCA)

EJBCA (Enterprise JavaBeans Certificate Authority) adalah salah satu sistem Infrastruktur Kunci Publik (PKI) terkemuka yang menawarkan ketahanan dan fleksibilitas tinggi. Dikembangkan oleh Tomas Gustavsson dan timnya pada tahun 2001, EJBCA telah menjadi sistem lintas-platform yang dapat disesuaikan untuk berbagai jenis organisasi. EJBCA tersedia dalam dua edisi: edisi Komunitas yang gratis dan open-source di bawah lisensi LGPL v2.1, serta edisi Enterprise yang menawarkan lebih banyak fungsionalitas dan dukungan (Garrido, 2024).

EJBCA menyediakan layanan otomatis untuk mengelola tugas-tugas penting dalam pemeliharaan PKI, seperti penerbitan sertifikat dan pembaruan Certificate Revocation List (CRL). Layanan ini dapat dikonfigurasi untuk berjalan secara berkala atau berdasarkan kondisi tertentu, sehingga memastikan kelancaran operasional PKI (Garrido, 2024).

2.2.6 Sertifikat Digital

Sertifikat digital berfungsi sebagai "paspor digital" yang unik dan tidak dapat dipalsukan, digunakan untuk memverifikasi identitas komputer, individu, atau organisasi dalam jaringan. Sertifikat ini memastikan keaslian dan legitimasi situs web serta pengguna dengan mengenkripsi dan

menandatangani identitas pemilik sertifikat yang dikeluarkan oleh Certificate Authority (CA) (Ferdous, 2022).

PKI, yang didukung oleh sertifikat digital, memperkuat kebijakan keamanan melalui protokol dan prosedur komunikasi, memungkinkan transaksi informasi rahasia secara aman di jaringan yang tidak aman. Dengan menggunakan CA pribadi seperti EJBCA, organisasi dapat mengelola proses penerbitan pasangan kunci kriptografi dan sertifikat publik mereka sendiri, memberikan kontrol penuh atas keamanan informasi (Ferdous, 2022).

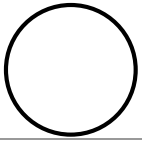
2.2.7 Context Diagram

Context Diagram (CD) adalah diagram yang mencakup sebuah proses dan memberikan gambaran suatu sistem. Sebagai level paling tinggi dalam Data Flow Diagram (DFD), diagram ini menampilkan seluruh input yang masuk ke sistem maupun output yang kemudian dihasilkan oleh sistem (Safwandi et al., 2021). CD menunjukkan sistem secara keseluruhan, di mana semua entitas eksternal harus digambarkan dengan jelas. Hal ini memungkinkan untuk melihat aliran data dari input, proses, hingga output, sehingga hubungan antara sistem dan lingkungan luarnya dapat terlihat (Soufitri, 2019).

2.2.8 Data Flow Diagram

Data Flow Diagram (DFD), atau yang sering disebut Diagram Arus Data (DAD), adalah sebuah model logis yang memvisualisasikan pergerakan data dalam suatu sistem. DFD berfungsi untuk menggambarkan sumber data, tujuan keluaran data dari sistem, tempat data disimpan, proses yang menghasilkan data, serta interaksi antara data yang tersimpan dan proses untuk mengolahnya (Kristanto, 2008, dikutip dalam Soufitri, 2019). Terdapat dua teknik utama dalam menggambarkan simbol DFD, yaitu metode Gane and Sarson dan metode Yourdon and De Marco (Soufitri, 2019). Dalam penelitian ini, metode Yourdon and De Marco juga dipilih sebagai pendekatan yang digunakan.

Tabel 2.2 Simbol Data Flow Diagram Yourdon and De Marco

Simbol	Keterangan
	External Entity Sumber yang berada di luar sistem yang sedang dikembangkan, seperti kantor, departemen, individu, organisasi, sumber transaksi, atau penerima laporan.
	Data Flow Aliran data yang terdiri seperti input dan output sistem. Arah panah untuk menggambarkan pergerakan aliran data yang masuk atau keluar dari suatu proses.
	***Process*** Tindakan atau tugas yang dijalankan oleh manusia, mesin, atau komputer, dengan menggunakan aliran data yang diterima dan menghasilkan aliran data yang dikeluarkan.
	Data Store Lokasi penyimpanan data, baik berupa file, database dalam sistem komputer, arsip manual, catatan fisik, tabel referensi, atau buku agenda.

2.2.9 Entity Relationship Diagram

Sitanggang (2013) menjelaskan ERD adalah metode pemodelan yang menggunakan diagram untuk menampilkan informasi tentang entitas, atributnya, serta hubungan antar entitas. ERD berfungsi untuk memvisualisasikan hubungan atau koneksi antara satu entitas dan entitas lainnya dalam sebuah sistem. Metode ini menggunakan struktur prosedur, alat, teknik, dan proses yang dirancang khusus untuk memodelkan hubungan tersebut (Nurmasari et al., 2023).

2.2.10 PIECES

Metode PIECES (Performance, Information, Economic, Control, Efficiency, dan Service) merupakan pendekatan yang digunakan dalam perancangan sistem untuk membandingkan proses antara sistem lama dengan sistem baru yang sedang dikembangkan (Oktaviani et al., 2021).