Journal
Peqguruang: Conference Series
eISSN: 2686–3472

JPCS
Vol. 3 No. 2 Nov. 2021

Graphical abstract

TANDA TANGAN DIGITAL BERBASIS ANDROID

[1]Adhyyaksa Alhady M.Ali, [2]Syarly, [3]Andi Ircham Hidayat
[1]Teknik Informatika, [2]Fakultas Ilmu Komputer,
[3]Universitas Al Asyariah Mandar

adhyaksaalhadym.ali@gmail.com
msyarli44@gmail.com
ircham.hdyt@gmail.com

Abstract

Signatures are used not only to maintain and ensure the authenticity of information but also to avoid denial from the parties involved. In cryptography, there is a concept called digital signature, which works similarly to signatures in general, one of which is the Schnorr algorithm. The Schnorr algorithm takes advantage of the discrete logarithm difficulty in signing and verifying it. The public and private key generation of the Schnorr algorithm requires a prime number generator algorithm, and the algorithm used in this study is the AKS algorithm. The process of signing and verifying the Schnorr algorithm requires a Hash function (SHA-1). The results showed that the average time for signing the Schnorr algorithm was 12.94 ms and 12.44 ms for the verification process.

Keywords: *Digital Signature, Android Digitala*

Abstrak

Tanda tangan tidak hanya digunakan untuk menjaga dan menjamin kredibilitas data tetapi juga untuk menghindari sumpah serapah dari pertemuan yang bersangkutan. Dalam kriptografi, ada ide yang disebut tanda tangan terkomputerisasi, yang bekerja sesuai dengan tanda sebagai aturan umum, salah satunya adalah perhitungan Schnorr. Perhitungan Schnorr memanfaatkan masalah logaritma diskrit dalam menandai dan memeriksanya. Masyarakat umum dan usia kunci pribadi dari perhitungan Schnorr membutuhkan perhitungan pembangkit bilangan yang tidak dapat dibagi, dan perhitungan yang digunakan dalam penyelidikan ini adalah perhitungan AKS. Cara paling umum untuk menandai dan mengonfirmasi perhitungan Schnorr membutuhkan pekerjaan Hash (SHA-1). Hasil penelitian menunjukkan bahwa waktu normal untuk menandai perhitungan Schnorr adalah 12,94 ms dan 12,44 ms untuk siklus cek.

Kata kunci: *Tanda Tangan Digital,Android Digital*

Article history
DOI: https://dx.doi.org/10.35329/jp.v3i2.2429
Received : *29 Juli 2021* | **Received in revised form :** *18 Agustus 2021* | **Accepted :** *28 September 2021*

1. PENDAHULUAN

Zaman sekarang ini dunia teknologi tetekomunikasi dan informasi berkembang dengan pesat. Salah satu pemicu utamanya adalah perkembangan teknologi internet yang banyak dipergunakan oleh penduduk dunia. Di Indonesia sendir pengguna internet mencapai 25 juta. Dengan Banyaknya pengguna internet akan semakin berpengaruh kehidupan sehari-hari. Selian itu kegiatan ekonomi semakin mudah dengan adanya internet.(Prasetiadi, 2017).

Tanda Tangan Digital DibangkitakanDari Hash Terhadap Pesan. Nilai HashAdalah Kode Ringkas Dari Pesan. Tanda Tangan DigitalBerlaku Seperti Tanda Tangan Dokumen Kertas.Tanda Tangan Digital Ditambahakan (Append) Pada Pesan.(Sulaiman .2017).

QR Kode (Quick Respone) Merupakan Bentuk Evaluasi Dari Barcode Yang Biasanya Kita Lihat Pada Sebuah Produk, QR Code Berbentuk Jajaran Persegi Berwarna Hitam Berbentuk Seperti Barcode Tetapi Dengan Tampilan Lebih Ringakas Yang Dapat Mempeoses Pertukaran Informasi Antar Mediah Lebih Cepat. QR Code BekerjaDengan Cara Yang Mirip Dengan Barcode UPC Dalam Data Yang Di Selenggarakan Dalam Bentuk Pola Yang Dapat diterjemahkan. (Nugraha, 2015)

Android SDK Merupakan Tools API (*Application Programming Interface*) Yang Dibutuhkan Untuk Mengawali Mengembangkan Aplikasi Pada Platform Android Menggunakan Bahasa Pemograman Java (Leksono & Nita, 2018).

Website Dapat Diartikan Sebagai Kumpulan Halaman-Halaman Yang Digunakan Untuk Mempublikasikan Informasi Berupa Text, Gambar, Dan Program Multimedia Lainnya Berupa Animasi, Suara, Dan Atau Gabungan Dari Semua Itu, Baik Yang Bersifat Statis Maupun Dinamis Yang Membentuk Satu Rangkaian Bangunan Yang Saling Terikat Antara Halaman Dengan Halaman Lainnya Yang Sering Disebut Sebagai *Hyperlink*. (Dwi Oktaviani, 2015)

Antarmuka Pengguna Android Didasarkan Pada Manipulasi Langsung, Menggunakan Masukan Sentuh Yang Serupa Dengan Tindakan Di Dunia Nyata, Seperti Menggesek, Mengetuk, Mencubit, Dan Membalikkan Cubitan Untuk Memanipulasi Obyek Di Layar. Android Adalah Sistem Operasi Dengan Sumber Terbuka, Dan Google Merilis Kodenya Di Bawah Lisensi Apache. Kodedengan Sumber Terbuka Dan Lisensi Perizinan Pada Android Memungkinkan Perangkat Lunak Untuk Dimodifikasi Secara Bebas Dan Didistribusikan Oleh Para Pembuat Perangkat, Operator Nirkabel, Dan Pengembang Aplikasi.Selain Itu, Android Memiliki Sejumlah Besar Komunitas Pengembang Aplikasi (Apps) Yang Memperluas Fungsionalitas Perangkat, Umumnya Ditulisdalam Versi Kustomisasi Bahasa Pemrograman Java. (Ferdiansyah Et Al., 2016)

Android merupakan subset perangkat lunak untuk perangkat mobile yang meliputi system operasi, middleware dan aplikasi inti yang direlease oleh Google. Android SDK (Software Development Kit) menyediakan Tools dan API yang diperlukan untuk mengembangkan aplikasi pada platform android dengan menggunakan bahasa pemrograman Java. (Rahman, A., Qashlim, A., & Anggita, D., 2021)

Berdasarkan dari peniltian diatas maka penulis mencoba melakukan penelitian yang serupa dengan munggunakan metode verifikasi QR-Code untuk melakukan autentik kebenaran kepemilikan tanda tangan tersebut.

2. METODE PENELITIAN

Makna metodologi sering diartikan berbeda antara satu peneliti dengan peneliti lainnya. Sering kali metodologi digunakan sebagai sinonim dari kata metode. Metode dapat diartikan sebagai cara berpikir, dengan demikian metodologi penelitian dapat diartikan sebagai pemahaman metode-metode penelitian dan pemahaman teknik-teknik penelitian. (Utami, E., Istiyanto, J. E., & Raharjo, S. 2007)

Adapun alat yang digunakan dalam perancanggan tanda tangan digitat (*Digital Signature)* yaitu :

a. Hardware (perangkat Keras)
   Dalam penelitian ini perangkat keras yang dibutuhkan untuk merancang tanda tangan digital (*digital signature)* yaitu komputer atau laptop yang memiliki spesifikasi minimal
b. Software (Perangkat Lunak)
   Tidak menutup kemungkinan spesifikasi Software akan berubah mengikuti kebutuhan sistem. Sehingga dalam penelitian ini membutuhkan perangkat lunak yaitu :

1. Sublime sebagai text editor
2. chrome/Mozilla Firefox sebagai web browser
3. Xampp v5 sebagai server local
4. MySQL sebagai databes

Adapun bahan yang digunakan yaitu

a. Tanda tangan
b. Persuratan desa

Waktu Dan Tempat

Penelitian ini dilaksanakan di Kantor desa Duampanua kecamatan anreapi kabupaten polewali mandar yang berlangsung pada bulan maret sampai Mei 2021.

Teknik pengumpulan data

Teknik pengumpulan data merupakan langkah yang paling strategis dalam penelitian, karena tujuan utama dari penelitian adalah mendapatkan data (Sugiyono, 2007: 62). Teknik pengumpulan data yang digunakan dalam penelitian ini adalah:

1. Observasi
   Pengumpulan data yang dilakukan dengan cara observasi yaitu melakukan pengmatan lansung pada lokasi penelitian atau pada suatu yang menjadi objek penelitian berupa penggunaan akhir atau menejemen pelayanan
2. Studi Pustaka
   Merupakan cara pengumpulan data dengan mempelajari literatur, paket modul paduan, buku-buku pedoman, buku-buku perpustakaan dan segala kepustkaan lainya yang dianggap perlu dan mendukung.

Teknik Analisis Data

Dalam melakukan analisis data pada penelitian ini, peneliti mengacu pada tahapan teknik analisis data menurut Miles dan Huberman dalam Herdiansyah, Haris (2010: 164) yaitu:

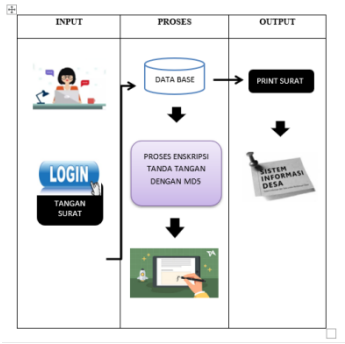
Menelaah Seluruh Data Yang Telah Diperoleh

1. Reduksi Data Adalah Merangkum , Memilih Hal-Hal Yang Pokok, Fokus Pada Target Informasi,Data Yang Tidak Perlu Disimpan Saja.
2. Penyusunan Satuan Dan Kategorisasi. Seluruh Data Yang Telah Diperoleh Bdiklasifikasikan Sesui Dengan Pokok Permasalahan

Penafsiran Data Yakni Menyampaikan Kesimpulan Dari Data-Data Yang Telah Diperoleh. Oleh Karena Itu Perlu Dicamtungkan Secara Eksplisit Dalam Desain.

Kerangka Sistem

Kerangka sistem dibawa menjelaskan secara bertahap tentang proses yang dilakukan sistem. Proses yang dilakukan sistem adalah sebagai berikut



Gambar: 1 Kerangka sistem

3. HASIL DAN PEMBAHASAN

Implementasi

Pada penelitian aplikasi ini dapat mengimplementasikan bahwa masyarakat dapat mengirimkan tandatangan atau mengcopy tanda tangan sehingga memudahkan masyarakat untuk file data desa

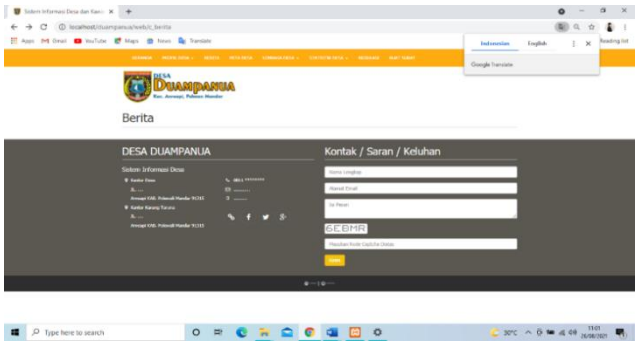
Gambar 2 Implementasi aplikasi

Pengujian Aplikasi

Dalam pembahasan ini saya akan menguraikan tentang bagaimana bendungan irigasi di website dan dapat menyelesaikan masalah yang ada yaitu :

1. Tampilan dasbor

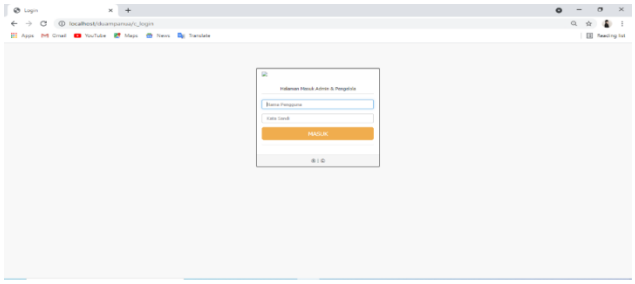
Pada tampilan dasboar aplikasi tanda tanga digital masyarakat dapat melihat menu-menu yang dapat diliahat atau dibuka seperti profil desa, lembaga desa, peta desa, dan pembuatan surat tanda tanga digital sehingga masyarakat dapat melihat isi dari aplikasi desa berbasis tanda tangan digital yang sangat membantu desa dalam penandatanganan surat masyarakat yang belum ditanda tangani oleh kepala desa sehingga masyarak dapat memasuki aplikasi agar memudahkan.



Gambar 3 Tampilan Dasbor

3. Tampilan buat surat

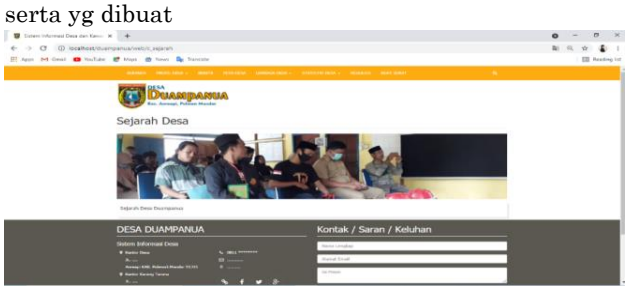
Pada tampilan buat surat pada gambar dibawa admin harus login terlebih dahulu agar dapat membuat surat yang dituju.



Gambar 4.4 Tampilan Bauat Surat

4. Tampilan Profil Desa

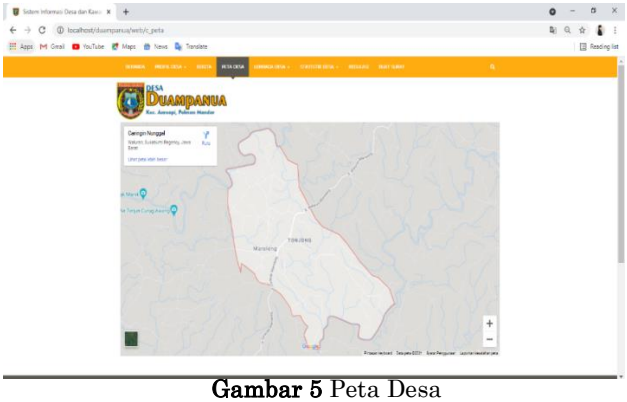
Kemudian pada tampilan profil desa kita dapat melihat profil desa seperti kegiatan desa yang perna diikuti serta yg dibuat



Gambar 4 Tampilan Dasbor

5. Peta Desa

Pada gambar dibawa kita bisa melihat bahwa tampilan peta desa agar msyarakat dapat melihat kondisi besar peta seluas apa dab dapat dilihat.



Gambar 5 Peta Desa

4. SIMPULAN

Keamanan dan pengklasifikasian data merupakan hal yang vital, berbagai hal telah dilakukan agar keamanan dan kerahasiaan data ini tetap terjaga dengan baik, Penggunaan aplikasi berbasis android dapat dimanfaatkan untuk memahami tanda tingkat lanjut (Computerized Mark) dengan merencanakan aplikasi yang menggunakan bahasa pemrograman PHP menggunakan teknik konfirmasi QR Code, serta menjaga keamanan dan privasi, juga diperlukan non-forswearing dengan memanfaatkan perhitungan tanda tangan terkomputerisasi (MD5) atau tanda tangan terkomputerisasi yang diharapkan dapat memeriksa apakah pesan atau data itu benar. Diperoleh dalam kondisi pertama penyampaian atau telah diubah sehingga pesan atau data itu tidak unik.

DAFTAR PUSTAKA

Dwi Oktaviani Program. (2015). Perancangan sistem informasi administrasi siswa pada smk bina utama kendal berbasi s web. *Perancangan Sistem Informasi Administrasi Siswa Pada Smk Bina Utama Kendal Berbasis Web*, *19*, 1–13.

Ferdiansyah, M. S., Informatika, J. T., Kampus, D., Tinggi, S., & Nurul, T. (2016). *APLIKASI QUICK RESPONSE DALAM MELAYANI PENGADUAN KERUSAKAN SARANA STT NURUL JADID BERBASIS ANDROID DAN*. *8*, 152–157.

Ferdiansyah1, M. S., Jasri., M., 2, & Widjianto3. (2016). Aplikasi Quick Response Dalam Melayani Pengaduan Kerusakan Sarana Stt Nurul Jadid Berbasis Android Dan Web. *Prosiding SENTIA*, *8*(Muhammad Soleh Ferdiansyah1, Mohammad Jasri. 2 , Widjianto3), 152–157.

Herdiansyah, Haris. 2010. *Metode Penelitian Kualitatif untuk Ilmu-ilmu Sosial.* Jakarta: Salemba Humanika.

Nugraha, M. P. (2011). *Pengembangan Aplikasi QR Code Generator dan QR Code Reader dari Data Berbentuk Image*.

Prasetiadi, A. E. (2011). *WEB 3 . 0 : TEKNOLOGI WEB MASA DEPAN*. *1*(3), 1–6.

Rahman, A., Qashlim, A., & Anggita, D. (2021). Teknologi Sistem Kontrol Untuk Pengelolaan Aktifitas Ruang Kelas. *Proceeding KONIK (Konferensi Nasional Ilmu Komputer)*, *5*, 74-79.

Sulaiman, O. K., Ihwani, M., & Rizki, S. F. (n.d.). *MODEL KEAMANAN INFORMASI BERBASIS TANDA TANGAN DIGITAL DENGAN DATA ENCRYPTION STANDARD (DES) ALGORITHM*. 14–19.

Sugiyono. 2007. *Metode Penelitian Kuantitatif Kualitatif* dan R&D. Bandung: Alfabeta.

Utami, E., Istiyanto, J. E., & Raharjo, S. (2007, November). Metodologi penelitian pada ilmu komputer. In *Seminar Nasional Teknologi 2007* (pp. 1-13).