Implementasi Hash untuk Verifikasi Keaslian Foto Bukti Transaksi QRIS

Ahmad Mutawalli - 13517026
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
13517026@std.stei.itb.ac.id

***Abstract*—Perkembangan pesat dari berbagai industri termasuk sektor finansial yaitu salah satu nya sistem pembayaran yang cashless. Untuk mendukung proses tersebut, diperlukan mekanisme untuk membuktikan bukti transaksi yang dikirimkan pembeli itu asli sehingga aman bagi penjual. Salah satu metode untuk membuktikan bukti transaksi tersebut valid adalah dengan menggunakan fungsi hash. Pada makalah ini akan dibahas mengenai implementasi kriptografi fungsi hash Keccak untuk mewujudkan transaksi cashless yang aman**

Keywords—fungsi hash, Keccak, bukti transaksi

I. Introduction (*Heading 1*)

Dengan pesatnya perkembangan industri dalam beberapa dekade terakhir, banyak sektor yang harus mengikuti perkembangan teknologi, salah satunya sektor finansial. Salah satu nya adalah pembayaran yang bersifat *cashless*. Bagi penjual yang melakukan kegiatan transaksi, penjual dapat meminta pembeli untuk melakukan pembayaran menggunakan metode *cashless* dan pembeli dapat mengirimkan bukti transaksi dalam bentuk foto.

Namun, foto bukti transaksi bisa diedit oleh pihak yang tidak berwenang. Foto bukti transaksi bisa menggunakan foto screenshot yang nominal telah diganti.

Oleh karena itu, pada makalah ini akan dibahas mengenai implementasi hash sebagai salah satu metode untuk meningkatkan keamanan pembayaran secara digital. Dengan menggunakan hash, maka setiap transaksi pembayaran akan terjamin autentik sesuai dengan prinsip dari hash.

II. LANDASAN TEORI

A. *Fungsi Hash Keccak*

Fungsi Keccak merupakan fungsi hash yang dikembangkan oleh Guido Breton, Joan Daemen, Michaël Peeters, dan Gilles Van Assche dan pertama kali dipublikasikan pada tahun 2015. Keccak menggunakan mekanisme konstruksi 'spons' atau sponge construction. Mekanisme konstruksi spons akan menyerap data dalam suatu sponge, untuk kemudian akan diperas dan dihasilkan message digest.

Secara umum, algoritma Keccak adalah sebagai berikut:

- Pesan yang akan diproses M akan ditambahkan bit-bit pengganjal atau padding menjadi string P sehingga habis dibagi rate
- Potong string P menjadi blok-blok yang berukuran rate-bit
- Inisialisasi state S dengan nilai nol sepanjang panjang blok (b)
- Fase penyerapan. Untuk setiap blok P:
    - Lakukan operasi XOR dengan r-bit pertama dari state S
    - Masukkan hasil ke dalam fungsi permutasi f sehingga dihasilkan state baru S
- Fase pemerasan:
    - Inisialisasi string kosong Z
    - Selagi panjang Z belum sama dengan panjang luaran (d), sambungkan r-bit pertama dari state S
    - Jika panjang Z masih belum sama dengan d, masukkan ke dalam fungsi permutasi f sehingga menghasilkan state baru S

B. *OCR (Optical Character Recognition)*

OCR adalah proses mengkonversi gambar menjadi teks yang dapat diproses oleh mesin. OCR bekerja dengan cara memindai dokumen dan mengenali pola huruf atau karakter yang ada di dalamnya.

Tahap pada OCR, yaitu:

- Preprocessing: Melakukan penyesuaian gambar agar lebih mudah dianalisis, seperti merotasi gambar, menghilangkan noda pada gambar, membersihkan kotak atau garis pada gambar
- Pengenalan teks: Pengenalan teks pada OCR adalah pencocokan pola dan ekstraksi fitur

III. Rancangan Solusi

Dalam penyelesaian permasalahan verifikasi keaslian foto bukti transaksi QRIS digunakan pendekatan fungsi hash dengan bantuan OCR untuk ekstrak informasi dari foto. Dengan menggunakan hash, informasi yang didapatkan dari OCR dapat dipastikan keasliannya (data integrity)

Fungsi hash yang digunakan adalah fungsi hash keccak dengan ukuran 256-bit (keccak-256). Panjang message digest

yang dipilih adalah 256-bit dengan pertimbangan keamanan dan kecepatan pemrosesan.

IV. Implementasi

Untuk implementasi, program ditulis dalam bahasa python dengan menggunakan kakas Crypto.Hash untuk algoritma Keccak dan pytesseract untuk OCR.

A. Ekstrak Informasi

Berikut adalah fungsi untuk ekstrak informasi dari image menggunakan OCR.

```
import pytesseract
from PIL import Image

def information_extraction(image_name):
    img = Image.open(image_name)

    text = pytesseract.image_to_string(img)

    array = text.split('\n')

    array = [line for line in array if line.strip()]

    # date, nominal, transaction_id
    return [array[2], array[4], array[7].replace('No.Transaksi
', '')]
```

B. Generate Hash

Berikut adalah fungsi untuk generate hash menggunakan Keccak

```
def generate_hash(date, nominal, transaction_id):
    keccak_hash = keccak.new(digest_bits=256)

    data = date + "|" + nominal + "|" + transaction_id
    # Convert the string to bytes
    data_bytes = data.encode('utf-8')

    # Update the hash object with the bytes of the data
    keccak_hash.update(data_bytes)

    # Get the hexadecimal digest of the hash
    return keccak_hash.hexdigest()
```

V. PENGUJIAN DAN PEMBAHASAN

A. Pengujian

Terdapat dua pengujian yang dilakukan yaitu pengujian dengan bukti pembayaran yang valid dan pengujian dengan bukti pembayaran yang tidak valid.

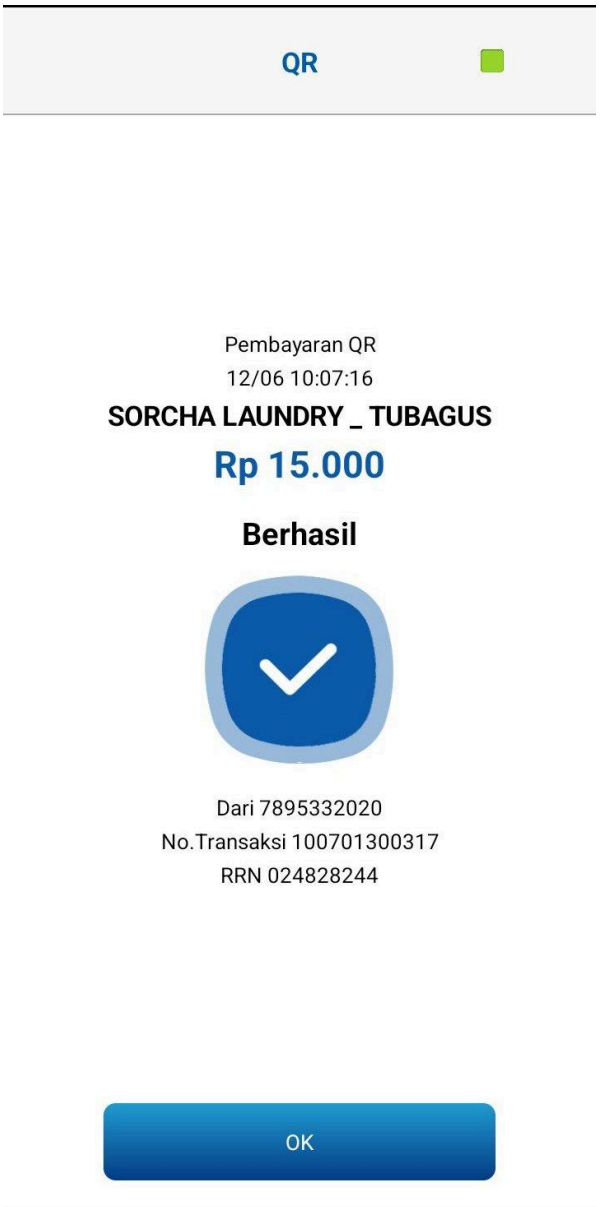
1. Pengujian dengan pembayaran yang valid

Lingkungan pengujian untuk kasus ini akan ditunjukan pada tabel berikut:

date	12/06 10:07:16
nominal	Rp 15.000
transaction id	100701300317

hash yang dihasilkan dengan lingkungan diatas adalah 1666989d0a155b9c184fdefd79a7658cb1062fbc3d349aed025e8b8f3ccf7dc3

Gambar yang akan divalidasi adalah sebagai berikut



Teks yang berhasil di ekstrak pada image tersebut adalah

QR B
Pembayaran QR
12/06 10:07:16
SORCHA LAUNDRY _ TUBAGUS
Rp 15.000
Berhasil
Dari 7895332020
No.Transaksi 100701300317
RRN 024828244

Setelah informasi didapatkan selanjutnya adalah melakukan hash pada informasi yang terkait transaksi yaitu waktu transaksi, nominal transaksi, dan id transaksi.

Hash yang dihasilkan pada image tersebut adalah 1666989d0a155b9c184fdefd79a7658cb1062fbc3d349aed025e8b8f3ccf7dc3

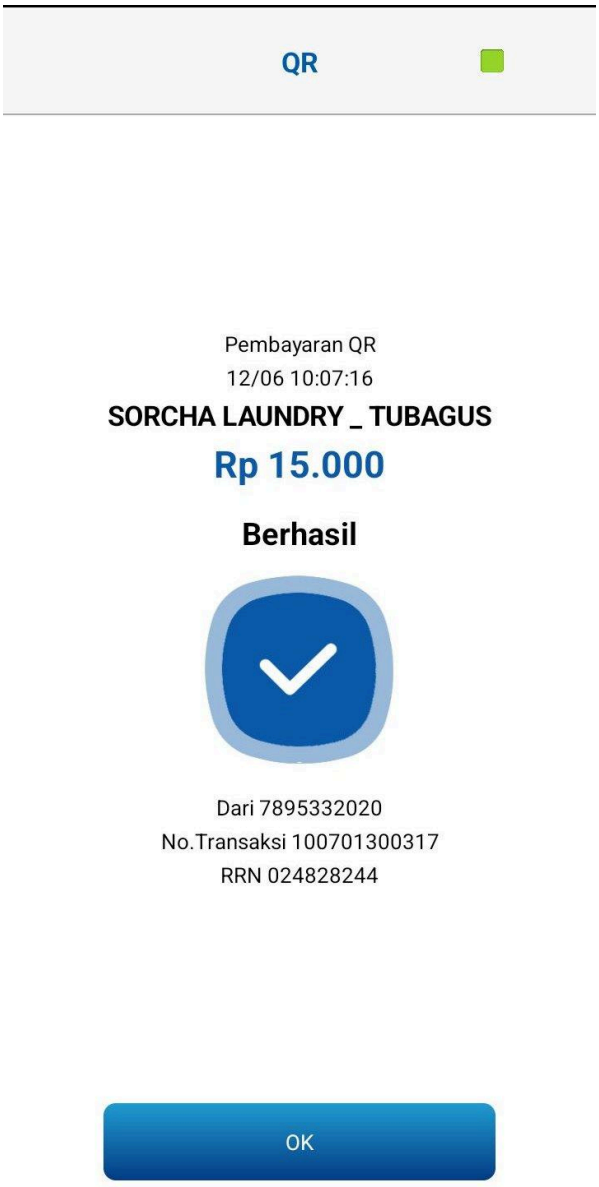
2. Pengujian dengan pembayaran yang tidak valid

Lingkungan pengujian untuk kasus ini akan ditunjukan pada tabel berikut:

date	12/06 10:07:16
nominal	Rp 20.000
transaction id	100701300317

hash yang dihasilkan dengan lingkungan diatas adalah 4a7edbe3bbd33ebc954f88d83ea4f8f3e6a0380a820123ae54d47417de5aa50b

Gambar yang akan divalidasi adalah sebagai berikut



Teks yang berhasil di ekstrak pada image tersebut adalah

QR B
Pembayaran QR
12/06 10:07:16
SORCHA LAUNDRY _ TUBAGUS
Rp 15.000
Berhasil
Dari 7895332020
No.Transaksi 100701300317

RRN 024828244

Setelah informasi didapatkan selanjutnya adalah melakukan hash pada informasi yang terkait transaksi yaitu waktu transaksi, nominal transaksi, dan id transaksi.

Hash yang dihasilkan pada image tersebut adalah 1666989d0a155b9c184fdefd79a7658cb1062fbc3d349aed025e8b8f3ccf7dc3

B. Pembahasan

Berdasarkan pengujian yang telah dilakukan, didapatkan hasil sebagai berikut:

1. Pengujian dengan pembayaran yang valid

   Informasi yang didapatkan pada gambar sesuai dengan kebutuhan yaitu tanggal transaksi, nominal transaksi, dan id transaksi. Hasil dari pengujian ini adalah sesuai dengan ekspektasi karena nilai hash dari transaksi dengan hash dari informasi yang didapatkan dari gambar sama

2. Pengujian dengan pembayaran yang tidak valid

   Informasi yang didapatkan pada gambar sesuai dengan kebutuhan yaitu tanggal transaksi, nominal transaksi, dan id transaksi. Hasil dari pengujian ini adalah sesuai dengan ekspektasi karena nilai hash dari transaksi dengan hash dari informasi yang didapatkan dari gambar tidak sama

VI. KESIMPULAN DAN SARAN PENGEMBANGAN

Solusi yang diimplementasikan berhasil untuk memastikan bukti pembayaran memenuhi aspek keasliannya (*data integrity*).

Kedepannya, solusi dapat dikembangkan lebih lanjut pada beberapa bagian seperti implementasi untuk berbagai jenis bukti pembayaran

UCAPAN TERIMAKASIH

Ucapan terimakasih penulis nyatakan kepada Tuhan Yang Maha Esa, karena karunia-Nya penulis bisa diberikan kesempatan untuk menyelesaikan dan bisa memberikan kontribusi nyata dalam memberikan ide yang dituliskan pada makalah ini.

Penulis juga mengucapkan terimakasih kepada Dr. Rinaldi Munir atas dedikasinya dalam memberikan ilmu pengetahuan tentang kriptografi kepada penulis.

REFERENSI

[1] Munir, Rinaldi "Fungsi Hash". https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/27-SHA-3-2024.pdf Diakses pada 12 Juni 2024

[2] AWS "What Is OCR (Optical Character Recognition)?" https://aws.amazon.com/id/what-is/ocr/ Diakses pada 12 Juni 2024

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Juni 2024

Ahmad Mutawalli 13517026