Bit (Fakultas Teknologi Informasi Universitas Budi Luhur) p-ISSN: 1693-9166
Vol. 20, No. 2, September 2023, hlm. 123-130 e-ISSN: 2685-127X

IMPLEMENTASI ALGORITMA HMAC-SHA-256 UNTUK KEAMANAN KEMASAN PRODUK

Bangga Angkasa[1*], Asriyanik[2], Agung Pambudi[3]

[1,2,3]Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Muhammadiyah Sukabumi
Email:[1*]bangga.angakasa@ummi.ac.id, [2]asriyanik263@ummi.ac.id, [3]agungpambd@ummi.ac.id

(*: Corresponding Author)

(Naskah masuk: 9 Agustus 2023, diterima untuk diterbitkan: 22 Agustus 2023)

Abstrak

Perkembangan teknologi memiliki dampak yang signifikan pada perindustrian, teknologi telah membantu perusahaan dalam meningkatkan efisiensi produksi, mengurangi biaya serta meningkatkan kualitas produk. Kemasan produk merupakan salah satu cara pemilik usaha menyiapkan informasi produk ke tangan konsumen. Namun pemalsuan label kemasan pada kemasan produk seperti perubahan tanggal kadaluwarsa atau juga peniruan Produk menjadi salah satu kendala dalam menjaga kualitas produk. Banyak upaya yang dilakukan dalam mencegah pemalsuan produk, salah satunya adalah dengan penggunaan segel hologram yang sulit dipalsukan, namun hal ini menyebabkan masalah baru dikarenakan pembuatan segel hologram membutuhkan mesin khusus dan biaya yang tidak sedikit. Untuk itu penelitian ini bertujuan untuk mengamankan produk menggunakan algoritma HMAC-SHA256 yang akan menjadi *alternative* segel keamanan kemasan produk. Algoritma HMAC-SHA256 yang merupakan algoritma hash yang memiliki kelebihan kecepatan komputasi dibandingkan dengan algoritma enkripsi, selain itu algoritma ini memiliki nilai *Avalanche effect* sebesar 68.24% yang dapat dikatakan baik karena persentase nilai lebih dari 50%. Hasil akhir dari penelitian ini adalah menciptakan sistem yang dapat membuat dan membuktikan segel keamanan kemasan untuk alternatif segel keamanan produk.

Kata kunci: *HMAC, Hash Kriptografi, Segel Keamanan, SHA-256*

IMPLEMENTATION OF HMAC-SHA-256 ALGORITHM FOR PRODUCT PACKAGING SECURITY

Abstract

Technology development has a significant impact on industry, technology has helped companies increase production efficiency, reduce costs and improve product quality. Product packaging is one of the ways business owners tell product information to the consumer. However, falsification of packaging labels on product packaging such as changes in expiration dates or product imitations is one of the obstacles in maintaining product quality. Many efforts have been made to prevent product counterfeiting, one of which is the use of holographic seals that are difficult to counterfeit, but this causes new problems because making holographic seals requires special machines and high costs. For this reason, this research aims to secure products using the HMAC-SHA256 algorithm which will be an alternative to product packaging security seals. The HMAC-SHA256 algorithm which is a hash algorithm that has the advantage of computational speed compared to encryption algorithms, besides this algorithm, has an Avalanche effect value of 68.24% which can be said to be good because the percentage value is more than 50%. The final result of this research is to build a system that can create and prove packaging security seals for alternative product security seals.

***Keywords**: QR-code seals, HMAC algorithm, SHA256 algorithm, product security seals.*

1. PENDAHULUAN

Kemasan produk merupakan salah satu cara pemilik usaha menyampaikan informasi produk ke tangan konsumen. Informasi yang tepat dan juga akurat menjadi hal penting yang harus dipertimbangkan oleh pemilik usaha, dikarenakan informasi produk menjadi salah satu sarana konsumen dalam mempertimbangkan suatu produk. Pemilik usaha juga harus menjaga informasi yang disampaikan oleh kemasan terjaga sampai ke tangan konsumen, namun pemalsuan kemasan seperti perubahan tanggal kadaluwarsa atau juga peniruan produk menjadi salah satu kendala dalam menjaga kualitas produk[1].

Pemalsuan tanggal kadaluwarsa pada produk di Indonesia sudah sering terjadi seperti yang

disampaikan kapolres Pasuruan, AKBP Rofiq Ripto Himawan mengungkapkan produk yang sudah kadaluwarsa diedarkan kembali oleh oknum yang tidak bertanggung jawab dengan cara menghapus tanggal kadaluwarsa yang sebenarnya dan diganti dengan cetakan tanggal kadaluwarsa yang baru [2]. Kasus pemalsuan tanggal kadaluwarsa terus terjadi seperti kasus yang dikutip dari jurnalpolisi.co.id pada tanggal 12 Oktober 2022 polsek Cikupa Polresta Tangerang polda ungkap kasus tindak pidana perlindungan konsumen dan pangan tentang pemalsuan tanggal kadaluwarsa kopi saset dan telah mengamankan 750 kopi saset yang diganti tanggal kadaluarsanya[3].

Berdasarkan studi berkala setiap lima tahun sekali, yang dilakukan oleh masyarakat Indonesia anti pemalsuan (MIAP), data hasil studi menunjukkan bahwa produk-produk sangat rentan dipalsukan dengan kategori makanan dan minuman sebesar 20%, dalam skala global nilai ekonomi dari kasus pemalsuan produk dan pembajakan pada tahun 2022 ini mencapai 2,3 triliun US *Dollar* seperti yang dilaporkan oleh *international trademark association* (inta) dan *the international chamber of commerce* [4]. Banyak upaya yang dilakukan dalam mencegah pemalsuan produk, salah satunya adalah dengan penggunaan segel hologram yang sulit dipalsukan, namun hal ini menyebabkan pembuatan segel hologram membutuhkan mesin khusus dan biaya yang tidak sedikit. Seperti yang diungkapkan oleh [5] bahwa segel hologram memiliki tingkat keamanan mendekati pengaman uang, segel hologram atau stiker hologram menggunakan teknologi modern yaitu *laser computer film* dengan master atau moldingnya terbuat dari baja sehingga harga moldingnya pun cukup mahal berkisar 6 sampai 8 juta. Oleh karena itu pemilik usaha membutuhkan alternatif cara dalam mengamankan produknya dan menjaga informasi tetap terjaga dari awal produksi hingga ketangan konsumen. Salah satunya dengan memanfaatkan teknologi *quick response code* (QR-Code). QR-Code merupakan kode dua dimensi yang dikembangkan dari kode batang (*barcode*). QR-Code awalnya bertujuan untuk menampung huruf kanji dan karakter kana yang tidak dapat ditampung oleh *barcode*[6]. Namun penggunaan QR-Code saja tidak dapat menjamin keaslian maupun kebenaran data.

Dalam kriptografi untuk membuktikan keaslian dan kebenaran data dapat dilakukan dengan menggunakan nilai *message authentication code* (MAC) salah satu jenis nilai mac yang dibuat dengan algoritma hash adalah HMAC-X (*key-hash message authentication code*) dengan X adalah algoritma hash yang digunakan seperti HMAC-MD5 atau HMAC-SHA1. Algoritma hash yang sering digunakan adalah MD5 dan SHA1 namun algoritma ini memiliki kekurangan rentan terhadap serangan *brute force* dan menyebabkan *collision attack*[7]. SHA2 merupakan pengembangan dari algoritma hash SHA1 dan sudah menjadi standar yang ditetapkan oleh *national institute of standards and technology* (NIST) pada tahun 2010, namun karena infrastruktur pada masa itu masih menggunakan SHA1, pemindahan ke SHA2 sulit dilakukan dan setelah ditemukan celah pada SHA1 di tahun 2017 penggunaan SHA1 berkurang dan mulai beralih ke SHA2. Keamanan pada nilai HMAC sangat sulit dipecahkan, karena penyerang harus mengetahui pasangan *text* dan kunci. Jika penyerang mengetahui kombinasi *text* yang digunakan, penyerang harus melewati keamanan dari fungsi hash yang digunakan [8]. Algoritma hash SHA256 dinilai memiliki kemampuan enkripsi dan kerumitan yang tinggi, untuk memecahkan nilai hash dibutuhkan jumlah percobaan sebanyak 2^{256} kali [9].

Dalam menghitung nilai mac terdapat beberapa algoritma yang dapat digunakan selain algoritma HMAC (*hash-based message authentication code*) yang menggunakan hash, algoritma cmac (*cipher-based message authentication code*) menggunakan *chipper*. Telah dilakukan penelitian oleh liao dengan membandingkan algoritma HMAC-SHA256 dengan algoritma CMAC-AES 128 pada beberapa perangkat dimana beliau mengungkapkan bahwa HMAC-SHA256 lebih unggul dan dapat bekerja dengan baik di semua perangkat yang diuji coba sedangkan CMAC-AES128 mengalami kegagalan pada 2 dari 4 device yang di uji coba karena membutuhkan sumber daya yang lebih, pada uji coba kecepat eksekusi algoritma HMAC-SHA256 menyelesaikan tugas dengan waktu 7.1ms sedangkan algoritma CMAC-AES128 menyelesaikan tugas dengan waktu 165.9ms[10].

Penelitian terdahulu sudah memberikan gambaran dari implementasi keamanan kriptografi dan berhasil menyelesaikan permasalahan yang sejenis. Penelitian terdahulu yang ditulis oleh antika lorien dan theophilus wellem dengan judul "implementasi sistem otentikasi dokumen berbasis quick response (QR) Code dan digital signature"[11], mengimplementasikan *digital signature* dengan QR-Code yang dapat membuktikan keaslian dan kebenaran pada dokumen tepatnya sertifikat. Namun metode *digital signature* yang digunakan dan dikombinasikan dengan algoritma rsa yang menambah beban komputasi pada saat pembuatan dan juga pembuktian.

Berdasarkan uraian yang sudah dijelaskan, peneliti bermaksud untuk melakukan penelitian dengan judul "implementasi algoritma HMAC-SHA256 untuk keamanan kemasan produk". Dengan melakukan penelitian ini peneliti mengharapkan dapat membantu penyelesaian masalah dengan cara mengamankan informasi penting pada kemasan produk menggunakan algoritma HMAC-SHA256 dengan hasil algoritma yang dikemas ke dalam QR-Code untuk memudahkan pemakaian.

2. METODE PENELITIAN

Penelitian ini bertujuan untuk mengamankan produk dengan membuat segel kemasan yang dapat

menjamin keaslian atau orisinalitas dari suatu produk. Untuk mencapai tujuan penelitian dibutuhkan suatu metode, metode yang digunakan dalam penelitian ini merupakan metode yang terdapat pada algoritma HMAC dengan algoritma *hash* SHA256 untuk mendapatkan nilai MAC. Adapun tahapan yang dilakukan dalam penelitian ini adalah sebagai berikut:

2.1 Studi Pendahuluan

Pada tahapan ini dilakukannya studi pendahuluan tentang algoritma HMAC dan SHA256 yang diperlukan pada penelitian. Studi penelitian dilakukan dengan cara mengkaji penelitian terdahulu dan dasar pengetahuan yang didapatkan dari sumber-sumber seperti jurnal, artikel dan buku.

2.2 Analisis kebutuhan keamanan pada segel keamanan kemasan produk

Pada tahapan ini dilakukan analisis terhadap segel keamanan kemasan produk, kelebihan serta kekurangan yang dimiliki segel keamanan kemasan produk yang biasa digunakan dan membandingkan dengan solusi segel keamanan kemasan produk menggunakan algoritma HMAC-SHA-256.

2.3 Proses pengamanan segel kemasan produk menggunakan algoritma HMAC-SHA-256

Pada tahap ini dijelaskan proses pengamanan segel kemasan produk dengan menggunakan algoritma HMAC-SHA-256 dengan melakukan simulasi perhitungan nilai MAC pada saat pembuatan serta pembuktian segel kemasan keamanan.

2.4 Implementasi algoritma ke dalam aplikasi

Pada tahapan ini dilakukan Implementasi algoritma ke dalam aplikasi, implementasi dilakukan dengan menggunakan bahasa pemrograman PHP dengan membangun algoritma yang disesuaikan dengan kebutuhan aplikasi agar dapat digunakan dalam pembuktian produk.

2.5 Pengujian algoritma HMAC-SHA-256

Pada tahapan ini dilakukan pengujian algoritma yang sudah diimplementasikan, pengujian dilakukan dengan melakukan pengujian pengukuran kecepatan algoritma dan pengujian keamanan menggunakan metode *Avalanche effect*.

2.6 Pengembangan aplikasi

Pada tahapan ini dilakukan pengembangan aplikasi dengan cara mengembangkan aplikasi web pengaman produk dengan segel kemasan menggunakan algoritma HAMC-SHA-256, aplikasi dikembangkan dengan menggunakan alat bantu seperti XAMPP dan *CodeIgniter*.

2.7 Pengujian aplikasi

Pengujian aplikasi dilakukan untuk menguji aplikasi terhadap skenario yang dapat terjadi, pengujian akan dilakukan pada tahap pembuatan segel dan pengujian keaslian segel. Segel yang diuji akan dibuat ke dalam beberapa skenario yang diharapkan dapat menjadi tolak ukur keberhasilan aplikasi.

3. HASIL DAN PEMBAHASAN

3.1 Analisis kebutuhan keamanan pada segel keamanan kemasan produk

Segel keamanan kemasan produk merupakan sarana kegiatan perdagangan dalam menjamin keaslian atau orisinalitas dari sebuah produk oleh pemilik usaha atau perusahaan terhadap konsumen. Proses penjaminan keaslian sebuah produk dapat dilakukan dengan berbagai cara, salah satu cara adalah dengan menggunakan segel keamanan kemasan produk. Segel keamanan kemasan produk biasa berbentuk stiker yang ditempelkan ke sebuah kemasan produk dari stiker sederhana seperti stiker logo usaha atau stiker yang lebih kompleks dengan hologram yang sulit dipalsukan[12].

Segel keamanan kemasan produk memiliki beberapa kekurangan dan kelebihan contohnya pada stiker logo usaha memiliki kemudahan serta minimnya modal yang harus dikeluarkan untuk mencetak stiker namun kemudahan dan minimnya modal dapat memberikan celah pada pemalsuan atau pembuatan kembali oleh oknum selain dari pihak perusahaan, sedangkan pada stiker hologram memiliki kelebihan sulitnya dalam pemalsuan atau pembuatan kembali oleh oknum selain dari pihak perusahaan dikarenakan tingginya tingkat kompleksitas produksi stiker namun tingginya tingkat kompleksitas berdampak pada besarnya modal yang harus dikeluarkan untuk mencetak stiker[13].

Maka dari itu penulis mengusulkan alternatif dalam pembuatan segel keamanan kemasan produk dengan menggunakan algoritma HMAC-SHA-256, karena segel keamanan kemasan produk yang dibuat dengan menggunakan algoritma HMAC-SHA-256 memiliki kelebihan tingkat kesulitan dalam pemalsuan dan minimnya modal yang harus dikeluarkan untuk mencetak stiker karena cara mencetaknya tidak jauh berbeda dengan stiker sederhana seperti stiker logo usaha.

3.2 Proses pengamanan segel kemasan produk menggunakan algoritma HMAC-SHA-256

Proses pengamanan segel kemasan produk menggunakan algoritma HMAC-SHA-256 adalah pengamanan informasi penting pada produk dengan menghitung nilai MAC, kemudian untuk membuktikan orisinalitas informasi penting pada produk dilakukan pembuktian keaslian nilai MAC.

3.2.1 Penghitungan nilai MAC

Algoritma HMAC-SHA-256 adalah algoritma menghitung nilai MAC dengan menggunakan fungsi *hash* kriptografi, fungsi *hash* kriptografi yang digunakan adalah SHA-256. Algoritma HMAC-SHA-256 pada dasarnya adalah

algoritma menghitung nilai MAC dengan proses dua kali *hashing* pesan menggunakan dua kunci yang sudah di maksimalkan nilai *hamming-distance*.

1. Menyiapkan pesan dan kunci

Pada tahap ini pesan dan kunci harus disiapkan terlebih dahulu, pesan yang digunakan merupakan data informasi penting pada produk serta data yang digunakan oleh aplikasi untuk mengenali pesan dan memproses pada tahap pembuktian.

Data yang menjadi pesan untuk pembuatan segel kemasan produk adalah informasi penting pada produk yang bersifat tidak statis atau informasi yang dicetak berbeda pada setiap produk, perusahaan biasanya menambahkan data ini ke dalam kemasan produk dengan alat cetak atau stempel yang menggunakan tinta, contoh pesan yang digunakan sebagai berikut:

a. *Manufacturing Identifier* (MFID)

Manufacturing identifier atau nomor produksi merupakan data yang berada pada produk, data ini merupakan data yang tidak statis atau data yang berubah setiap produk dibuat. MFID biasa digunakan oleh perusahaan sebagai nomor serial atau nomor jumlah produksi.

b. *Mmanufacturing Date* (MFG)

Manufacturing date atau tanggal produksi merupakan data yang berada pada produk, data ini merupakan data yang tidak statis atau data yang berubah setiap produk dibuat. MFG biasa digunakan oleh perusahaan dalam memberi tahu tanggal produk dibuat.

c. *Expired Date* (EXP)

expired date atau tanggal kedaluwarsa merupakan data yang berada pada produk, data ini merupakan data yang tidak statis atau data yang berubah setiap produk dibuat. EXP biasa digunakan oleh perusahaan dalam memberi tahu batas aman konsumsi produk.

Adapun data tambahan yang digunakan dalam pembuatan pesan untuk pembuatan segel kemasan produk, data tambahan yang digunakan adalah sebagai berikut:

a. *Key-unique identifier* (KUID)

Key-unique identifier adalah data yang berasal dari aplikasi, data ini merupakan nomor identitas yang bisa digunakan dalam pencarian kunci, produk dan pemilik. KUID digunakan sebagai lapisan keamanan agar segel keamanan tidak memiliki data penting seperti kunci yang dapat digunakan untuk menghitung nilai MAC.

b. *QR count* (QRC)

QR count adalah data yang dibuat oleh aplikasi untuk menandai segel ke berapa yang sedang dibuat, data ini juga berfungsi sebagai label pada segel agar mudah digunakan dan menjadi pembeda yang jelas.

Setelah pesan dibuat aplikasi dapat menentukan kunci, kunci ditentukan dari basis data produk yang ada di dalam aplikasi melalui KUID yang digunakan. Selanjutnya pesan dan kunci harus disederhanakan terlebih dahulu, dikarenakan tipe data atau karakter yang tidak sesuai dapat menggagalkan perhitungan atau pembuktian nilai MAC pada tahap-tahap selanjutnya. Berikut merupakan contoh pesan dan kunci yang akan digunakan pada simulasi perhitungan nilai MAC:

```
Pesan:
{
    "KUID": "4tNdA",          //Key-unique identifier
    "QRC": "U0012",           //QR count
    "MFID": "#0001",          //manufacturing identifier
    "MFG": "2023-05-02",      //manufacturing date
    "EXP": "2023-05-09"       //expired date
}
"KUID": "4tNdA" -> Kunci: keyprod1
```

Gambar 1. Data label kemasan

2. Membangkitkan kunci ipad dan kunci opad

Proses pembangkitan kunci dalam bentuk ipad dan opad dilakukan dengan melakukan operasi XOR antara setiap bit kunci dengan nilai ipad dan opad. Nilai ipad dan opad dalam algoritma HMAC adalah konstan atau sudah ditetapkan dan berubah sesuai dengan besar block yang digunakan oleh algoritma hash. Nilai ipad adalah “00110110” (36 dalam *hexadecimal*) dan opad adalah “01011100” (5C dalam hexadecimal) yang akan diulang sesuai dengan ukuran blok hash yang digunakan. Karena algoritma hash yang digunakan adalah SHA256 maka besar blok adalah 512 maka pengulangan nilai ipad dan opad akan diulang sebanyak 64 kali atau 512/8.

3. *Hashing* pertama pada kunci ipad digabung dengan pesan

Hashing pertama dengan algoritma SHA256 dilakukan dengan cara menggabungkan pesan dengan kunci ipad, penggabungan kunci ipad digabungkan pada awal pesan.

4. *Hashing* kedua pada kunci opad digabung dengan hasil *hashing* pertama

Hasing kedua dengan algoritma SHA256 dilakukan pada hasil hashing pertama digabung Dengan kunci opad, kunci opad digabungkan pada awal pesan.

3.2.2 Pembuktian nilai MAC

Pada tahap ini akan dilakukan simulasi pembuktian nilai MAC, transaksi nilai MAC dilakukan dengan cara mengirimkan pesan serta nilai MAC dari pesan itu sendiri. Untuk mengetahui kunci yang digunakan untuk menghitung nilai MAC maka

di dalam pesan akan ada tanda atau petunjuk untuk mencari kunci yang digunakan.

1. Mencari kunci

Untuk mencari kunci yang digunakan dalam perhitungan MAC terdapat nilai KUID (*key unique identifier*), nilai KUID ini dapat digunakan untuk mencari kunci pada basis data yang digunakan dalam menghitung nilai MAC sebelumnya.

2. Menghitung kembali nilai MAC

Setelah kunci didapatkan maka akan dihitung kembali nilai MAC dari pesan dan kunci dengan menggunakan algoritma HMAC-SHA-256 seperti yang sudah dilakukan pada tahap sebelumnya.

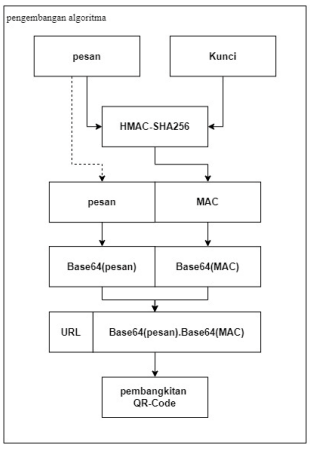
3. Menyamakan nilai MAC yang dihitung dengan nilai MAC dari pesan

Setelah nilai MAC yang baru sudah dihitung maka penyamaan nilai MAC awal dengan nilai MAC baru. Jika nilai MAC sama maka dapat dipastikan pesan belum diubah dan pesan berasal dari sumber yang diketahui, jika nilai MAC tidak sama maka dapat dipastikan ada pesan yang diubah atau kunci berasal dari pihak yang tidak diketahui.

3.3 Implementasi algoritma ke dalam aplikasi

Pada tahapan ini algoritma HMAC-SHA256 akan diimplementasikan dan disesuaikan dengan kebutuhan aplikasi, agar aplikasi berjalan sesuai dengan yang direncanakan maka diperlukan rancangan yang memenuhi kebutuhan, berikut merupakan alur pengembangan algoritma yang telah dibuat:

3.3.1 Implementasi algoritma HMAC-SHA-256



Gambar 2. Rancangan implementasi algoritma HMAC-SHA-256

Setelah rancangan alur implementasi algoritma HMAC-SHA-256 dibuat, langkah selanjutnya adalah mengubah alur ke dalam kode program menggunakan bahasa pemrograman PHP, berikut adalah potongan kode program HMAC-SHA-256 yang telah dibuat menggunakan bahasa pemrograman PHP.

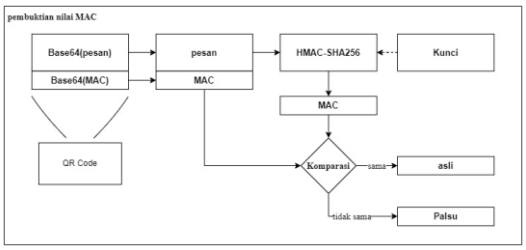
```
public function QRgeneratorMake($message,$key)
{
helper('hmacSha256');
$message = base64_encode_url(json_encode($message));
$mac=
base64_encode_url(hmac_sha256($message,$key['qrkey']));

$QRcode = Builder::create()
        ->writer(new PngWriter())
        ->writerOptions([])
        ->data(base_url().'/QRvalidate/'.$message.'.'.$mac)
        ->encoding(new Encoding('UTF-8'))
        ->errorCorrectionLevel(new
ErrorCorrectionLevelLow())
        ->size(300)
        ->margin(10)
        ->roundBlockSizeMode(new
RoundBlockSizeModeEnlarge())
        ->validateResult(false)
        ->build();

return $QRcode->getDataUri();
}
```

Gambar 3. Implementasi algoritma HMAC

3.3.2 Implementasi pembuktian nilai MAC



Gambar 4. Rancangan pembuktian nilai MAC

Setelah rancangan alur pembuktian nilai MAC dibuat, langkah selanjutnya adalah mengubah alur ke dalam kode program menggunakan bahasa pemrograman PHP, berikut adalah potongan kode program pembuktian nilai MAC yang telah dibuat menggunakan bahasa pemrograman PHP.

```
public function QRvalidatorMake($path)
{
 helper('hmacSha256');
 try
 {
  $qrcode = new QrReader($path);

  $qrpayload = $qrcode->text();
  $qrpayload = explode('.', substr($qrpayload,
strlen(base_url().'/QRvalidate')));

  $message =
(array)json_decode(base64_decode($qrpayload[0]));
  $key    = getKey($message['KUID']);
  }
  catch(\Exception $e){
  return 0
  }

$mac =
base64_encode_url(hmac_sha256($qrpayload[0],$key['qrkey']));
 if($qrpayload[1] != $mac) return 0;
 return 1;
}
```

Gambar 5. Implementasi pembuktian nilai MAC pada bahasa pemrograman PHP

3.4 Pengujian algoritma HMAC-SHA-256

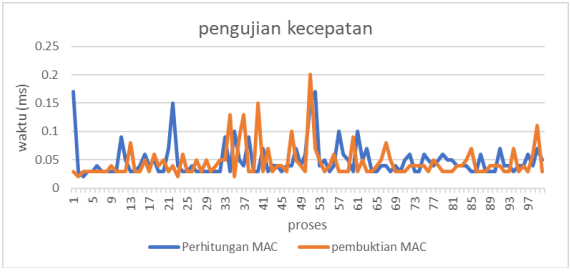
Pengujian algoritma dilakukan dengan beberapa cara yang bertujuan untuk menguji efektivitas algoritma, pengujian pertama dilakukan dengan cara mengukur kecepatan perhitungan nilai MAC serta pembuktian nilai MAC, pengujian kedua

melakukan pengujian *Avalanche effect* atau tingkat pengacakan algoritma kriptografi.

3.4.1 Pengukuran kecepatan

Dalam pengukuran kecepatan algoritma HMAC-SHA-256 digunakan fungsi dari bahasa pemrograman PHP, dimana dengan menghitung waktu proses fungsi berakhir dikurangi dengan waktu dimulainya proses perhitungan nilai MAC dan pembuktian nilai MAC. Adapun sampel yang digunakan merupakan data acak sesuai dengan susunan data yang digunakan pada aplikasi. Tahapan yang akan diuji adalah pengulangan masing-masing proses sesuai dengan sampel pesan dan kunci.

Berikut adalah hasil pengujian kecepatan pada proses perhitungan nilai MAC dan pembuktian nilai MAC serta hasil pengukuran dari masing-masing proses.



Gambar 6. Grafik pengujian kecepatan

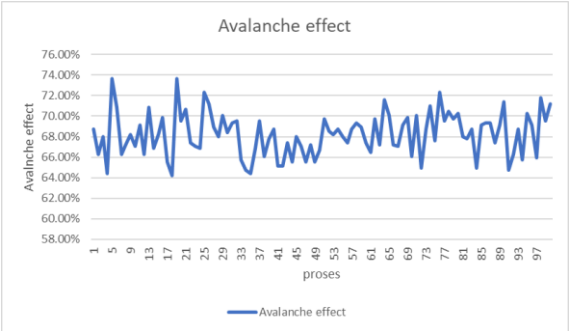
Berdasarkan hasil pengujian kecepatan pada gambar 6, didapatkan hasil kecepatan dari keseluruhan proses perhitungan nilai MAC dengan hasil rata-rata 0.049ms dan memiliki kecepatan pada proses tertinggi 0.17ms dan terendah 0.02ms. Sedangkan pada proses pembuktian nilai MAC didapat hasil rata-rata 0.046ms dengan kecepatan pada proses tertinggi 0.2ms dan terendah 0.02ms.

3.4.2 Avalanche effect

Avalanche effect merupakan pengujian dimana sedikit perubahan pada *input* dapat merubah sebagian besar dari output. Jika suatu fungsi kriptografi tidak memiliki nilai *Avalanche effect* yang baik, maka fungsi kriptografi tersebut memiliki pengacakan yang buruk dan berdampak pada kemudahan prediksi input hanya dari output yang dihasilkan. Nilai dari *Avalanche effect* yang baik adalah perubahan sedikit pada input mengakibatkan pengacakan yang besar kurang lebih adalah 50%. *Avalanche effect* dapat dihitung dengan menggunakan persamaan sebagai berikut:

$$AE = \frac{jumlah\ bit\ berubah}{jumlah\ bit\ total} \times 100\% \quad \text{.....(1)}$$

Di bawah ini merupakan hasil membandingkan dua hash dari pasangan pesan dan kunci yang dirubah untuk menghitung persentase nilai *avalanche effect* dari algoritma HMAC-SHA-256. Adapun sampel yang digunakan merupakan data acak sesuai dengan susunan data yang digunakan pada aplikasi.

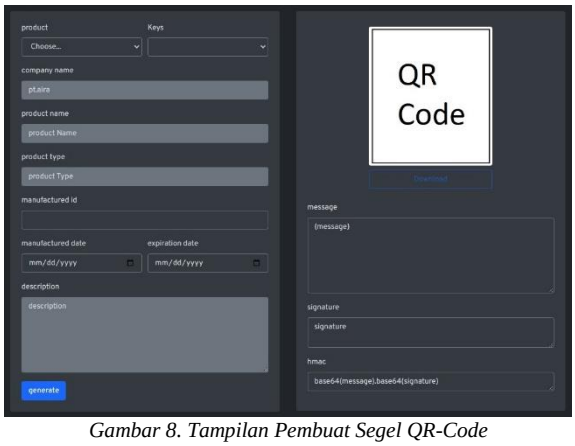


Gambar 7. Grafik pengujian Avalanche effect

Setelah melakukan perbandingan antara 100 pasangan nilai hash, didapatkan nilai perbandingan berdasarkan pada gambar 7, dengan hasil rata-rata *Avalanche effect* dari algoritma HMAC-SHA-256 sebesar 68.24%. Sesuai dengan yang sudah disampaikan sebelumnya, algoritma yang baik memiliki nilai pengacakan lebih besar dari 50%.

3.5 Pengembangan aplikasi

Setelah Algoritma HMAC-SHA256 di implementasikan maka tahap selanjutnya adalah mengembangkan algoritma yang sudah di implementasi ke dalam web, dimana web yang dikembangkan akan berfungsi sebagai pembuat QR-Code serta pembuktian QR-Code yang sudah dibuat, beberapa fitur akan dikemas ke dalam dua halaman yang akan mewakili proses pembuatan QR-Code oleh pemilik usaha serta pembuktian QR-Code oleh pembeli produk untuk membuktikan keaslian dari produk. Sebagai gambaran berikut adalah rancangan tampilan yang telah dikembangkan

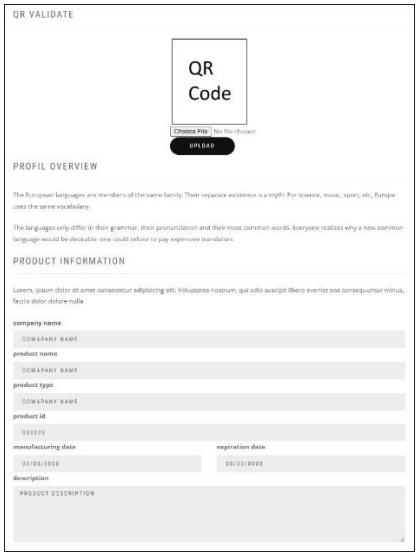


Gambar 8. Tampilan Pembuat Segel QR-Code

3.6 Pengujian aplikasi

Setelah Algoritma berhasil di kembangkan ke dalam web, maka web akan diuji untuk memastikan dapat digunakan dan berfungsi seperti yang sudah direncanakan. Pengujian akan dilakukan dengan melakukan unit testing dimana pada tiap-tiap fitur yang sudah diimplementasikan akan diberikan kasus

uji dan harapan hasil untuk memastikan fitur sudah dibuat seperti yang direncanakan.



Gambar 9. Tampilan Pembuktian Segel QR-Code

1. Pengujian fitur pembuat segel keamanan QR-Code

Tabel 1. Pengujian fitur pembuat segel keamanan QR-Code

No	Kasus uji	Harapan hasil	Hasil pengujian
1	Semua input valid	segel keamanan QR-Code berhasil dibuat	segel keamanan QR-Code berhasil dibuat
2	Tidak memasukkan input	Memberikan peringatan kesalahan 'tidak memasukkan input'	Memberikan peringatan kesalahan 'tidak memasukkan input'
3	Tidak memilih kunci	Memberikan peringatan kesalahan 'tidak memilih kunci'	Memberikan peringatan kesalahan 'tidak memilih kunci'
4	Salah memilih kunci	Memberikan peringatan kesalahan 'salah memilih kunci'	Memberikan peringatan kesalahan 'salah memilih kunci'
5	Tidak memilih produk	Memberikan peringatan kesalahan 'tidak memilih produk'	Memberikan peringatan kesalahan 'tidak memilih produk'
6	Salah memilih produk	Memberikan peringatan kesalahan 'salah memilih produk'	Memberikan peringatan kesalahan 'salah memilih produk'

Dari hasil pengujian pada tabel 1, fitur pembuat segel keamanan QR-Code yang dibuat sudah berhasil memenuhi setiap kasus uji.

2. Pengujian fitur pembuktian segel keamanan QR-Code

Tabel 2. Pengujian fitur pembuktian segel keamanan QR-Code

No	Kasus uji	Harapan hasil	Hasil pengujian
1	segel keamanan QR-Code yang dimasukkan sesuai	segel keamanan QR-Code asli	segel keamanan QR-Code asli
2	Isi segel keamanan QR-Code tidak sesuai	segel keamanan QR-Code tidak sesuai dan berkemungkinan besar palsu	segel keamanan QR-Code tidak sesuai dan berkemungkinan besar palsu
3	Salah memasukkan format gambar	segel keamanan QR-Code tidak sesuai	segel keamanan QR-Code tidak sesuai
4	Signature pada segel keamanan QR-Code salah	segel keamanan QR-Code palsu	segel keamanan QR-Code palsu

Dari hasil pengujian kasus uji pada tabel 2, fitur pembuktian segel keamanan QR-Code yang dibuat sudah berhasil memenuhi setiap kasus uji.

4. KESIMPULAN

Berdasarkan hasil dari tahapan penelitian yang sudah dilakukan dalam implementasi algoritma HMAC-SHA-256 untuk keamanan kemasan produk, maka dapat disimpulkan bahwa algoritma HMAC-SHA-256 dapat menjamin integritas serta keaslian informasi pada kemasan produk, dengan pengujian menggunakan data sampel sebanyak 100 data menghasilkan nilai rata-rata waktu pengerjaan pada proses perhitungan nilai MAC sebesar 0.049ms serta pada proses pembuktian nilai MAC sebesar 0.046ms, adapun hasil dari pengujian *Avalanche effect* dengan menggunakan data pengujian yang sama mendapatkan nilai rata-rata sebesar 68.24% yang dapat dikatakan baik karena persentase nilai lebih dari 50%.

Implementasi algoritma HMAC-SHA-256 pada keamanan kemasan produk telah berhasil dikembangkan pada website yang dapat digunakan untuk membuat serta membuktikan integritas informasi serta keaslian dari segel keamanan kemasan produk, berdasarkan pengujian fitur dengan skenario yang mungkin terjadi dapat disimpulkan implementasi algoritma HMAC-SHA-256 pada keamanan kemasan produk berjalan dengan baik dan menjadi alternatif dalam pembuatan segel keamanan kemasan.

DAFTAR PUSTAKA

[1] S. Lasmadi, E. Sudarti, and D. Wahyudhi, “Peningkatan Pemahaman Tentang Pemalsuan Label dan Iklan Makanan Guna Perlindungan

Konsumen Kepada Masyarakat Desa Danau Kedap Kabupaten Muaro Jambi," *Jurnal Karya Abdi Masyarakat*, vol. 6, no. 2, pp. 191–199, 2022.

[2] A. M. Memorandum, "Polres Pasuruan Bongkar Peredaran Crimer Susu Kadaluarsa - Memorandum.co.id." May 2021. [Online]. Available: https://memorandum.co.id/polres-pasuruan-bongkar-peredaran-crimer-susu-kadaluarsa/

[3] Grinaldi, "Press Conference Polsek Cikupa Tentang Kasus Tindak Pidana Perlindungan Konsumen Dan Pangan - jurnal polisi." Oct. 2022. [Online]. Available: https://jurnalpolisi.co.id/2022/10/12/press-conference-polsek-cikupa-tentang-kasus-tindak-pidana-perlindungan-konsumen-dan-pangan/

[4] M. Defitri, "Produk Palsu Sebabkan Indonesia Rugi Ratusan Triliun!," *Waste4Change*. Sep. 2022. [Online]. Available: https://waste4change.com/blog/produk-palsu-sebabkan-indonesia-rugi-ratusan-triliun/

[5] M. K. Idrizon, "Teknologi Hologram," *Perpustakaan Universitas Negeri Padang*. [Online]. Available: http://pustaka.unp.ac.id/read/artikel/13/teknologi-hologram–.html

[6] F. Ariyanto and S. Suprihadi, "Implementasi Digital Signature Dan Quick Response Code Pada Aplikasi Kuitansi Digital," *Jurnal Informatika dan Komputer*, vol. 5, no. 2, pp. 125–131, 2022.

[7] Y. Anugrah, M. H. H. Ichsan, and A. Kusyanti, "Implementasi Algoritme SHA-256 Menggunakan Protokol MQTT pada Budidaya Ikan Hias," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, vol. 2548, p. 964X, 2019.

[8] W. Stallings, *Cryptography and network security: Principles and practice, global edition*, 8th ed. London, England: Pearson Education, 2022.

[9] I. Rahim, N. Anwar, A. M. Widodo, K. K. Juman, and I. Setiawan, "Komparasi Fungsi Hash Md5 Dan SHA256 Dalam Keamanan Gambar Dan Teks," *ikraith-informatika*, vol. 7, no. 2, pp. 41–48, 2023.

[10] C.-H. Liao, "Message Authentication Codes On Ultra-Low SWaP Devices," Virginia Tech, 2022.

[11] A. Lorien and T. Wellem, "Implementasi Sistem Otentikasi Dokumen Berbasis Quick Response (QR) Code dan Digital Signature," *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, vol. 5, no. 4, pp. 663–671, 2021.

[12] M. K. Idrizon, "Teknologi Hologram," *Perpustakaan Universitas Negeri Padang*. [Online]. Available: http://pustaka.unp.ac.id/read/artikel/13/teknologi-hologram–.html

[13] S. Digibook, "Stiker Security Label Percetakan Stiker Semarang," *Digibook Promotion*. Apr. 2023. [Online]. Available: https://digibook.id/blog/stiker-security-label-percetakan-stiker-semarang/