Techno, ISSN 1410 - 8607
Volume 18 No. 1, April 2017
Hal. 059 – 068

TANDA TANGAN DIGITAL MENGGUNAKAN QR CODE DENGAN METODE ADVANCED ENCRYPTION STANDARD

Digital Signature Using QR Code By Advanced Encryption Standard Method

Abdul Gani Putra Suratma[1], Abdul Azis[2*]
[1] Program Studi Magister Ilmu Komputer , Program Pascasarjana,
Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama,
Jakarta Selatan 12260 Telp. (021) 5853753, Fax. (021) 5869225
[2] STMIK Amikom Purwokerto
Jl. Let. Jend. Pol. Sumarto Purwokerto
*Email: [2] abdazis9@gmail.com

ABSTRAK

Tanda tangan digital *(digital signature)* adalah sebuah skema matematis yang secara unik mengidentifikasikan seorang pengirim, sekaligus untuk membuktikan keaslian dari pemilik sebuah pesan atau dokumen digital, sehingga sebuah tanda tangan digital yang *autentik* (sah), sudah cukup menjadi alasan bagi penerima un- tuk percaya bahwa sebuah pesan atau dokumen yang diterima adalah berasal dari pengirim yang telah diketahui. Perkembangan teknologi memungkinkan adanya tanda tangan digital yang dapat digunakan untuk melakukan pembuktian secara matematis, sehingga informasi yang didapat oleh satu pihak dari pihak lain dapat diidentifikasi untuk memastikan keaslian informasi yang diterima. Tanda tangan digital merupakan mekanisme otentikasi yang memungkinkan pembuat pesan menambahkan sebuah kode yang bertindak sebagai tanda tangannya. Tujuan dari penelitian ini menerapkan *QR Code* atau yang dikenal dengan istilah *QR (Quick Respon)* dan Algoritma yang akan ditambahkan yaitu AES *(Advanced Encryption Standard)* sebagai tanda tangan digital sehingga hasil dari penelitian penerapan *QR Code* menggunakan algoritma *Advanced Encryption Standard* sebagai tanda tangan digital dapat berfungsi sebagai otentikasi tanda tangan pimpinan serta ve- rivikasi dokumen pengambilan barang yang sah. dari penelitian ini akurasi klasifi- kasi *QR Code* dengan menggunakan *naïve bayes classifier* sebesar 90% dengan *precision* positif sebesar 80% dan *precision* negatif sebesar 100%.

Kata kunci : *Digital Signature, QR Code, Kriptografi, AES, Security Validation*

ABSTRACT

signature is a schematic mathematically that uniquely identifies a sender , as well as to prove the authenticity of the owner of a message or document digi- tally, so that a digital signature is authentic (valid), is reason enough for the re- cipient to believe that a message or documents received are coming from un- known senders. The development of technology enabling their digital signature that can be used to prove mathematically, so that the information obtained by one party from the other party can be identified to ensure the authenticity of the in- formation received. The digital signature is an authentication

mechanism that al- lows the manufacturer to add a code message that acts as a signature. The pur- pose of this study apply the QR Code or which is known as QR (Quick Response) and algorithms to be added , namely AES (Advanced Encryption Standard) as a digital signature so that the results of the research application of the QR Code using Advanced Encryption Standard algorithm as a signature can function as a digital signature authentication and verification of document retrieval leaders le- gitimate goods . This research classification accuracy of the QR Code using a na- ïve Bayes classifier with a precision of 90% positive and 80% negative precision of 100% .

Keywords *: Digital Signature, QR Code, Kriptografi, AES, Security Validation.*

PENDAHULUAN

Perkembangan teknologi khususnya teknologi informasi dan komunikasi membawa perubahan yang mencakup seluruh peralatan teknis untuk memproses dan menyampaikan informasi. Dalam teknologi informasi dan komunikasi, per-tukaran proses data merupakan satu hal yang akan menjadi bagian yang sangat penting, karena saat ini seiring dengan perkembangan teknologi segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, pemindahan informasi antar media dapat dilakukan secara cepat dan berkualitas. Tanda tangan digital adalah satu tandatangan elektronik yang dapat digunakan untuk membuktikan keaslian identitas pengirim dari suatu pesan atau penandatangan dari suatu dokumen, dan untuk memastikan isi dari pesan atau dokumen dikirim tanpa perubahan. Pengisian *form* dokumen permintaan yang harus ditandatangani basah oleh pimpinan masih menggunakan sistem manual yang mengharuskan mencetak dokumen permintaan dan meminta tandatangan dari pimpinan. Kemudian untuk keperluan verifikasi dokumen, dokumen harus di *scan* dan mengunggahnya ke *server* pusat. Banyaknya dokumen yang harus ditandatangani dan pimpinan yang sering pergi keluar mengakibatkan proses tanda tangan membutuhkan waktu yang cukup lama sehingga membuat operasional sering terganggu. Tanda tangan digital tidak mudah ditiru oleh orang lain, dan dapat secara otomatis dilakukan *time stamp*. Kemampuan tanda tangan digital dapat memastikan bahwa pesan asli tidak bisa dengan mudah diganti.

Hadirnya teknologi baru *QR Code* (Quick Response) 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 ringkas yang dapat memproses pertukaran informasi antar media lebih cepat. QR *Code* bekerja dengan cara yang mirip dengan *barcode UPC* dalam data yang diselenggarakan dalam bentuk pola yang dapat diterjemahkan. Untuk menerapkan QR *Code* sebagai tanda tangan digital akan dipergunakan suatu ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi, integritas suatu data, serta otentikasi data yaitu kriptografi. Salah satunya kita dapat menggunakan algoritma *AES* (*Advanced Encryption Standard*). AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik..

METODE PENELITIAN

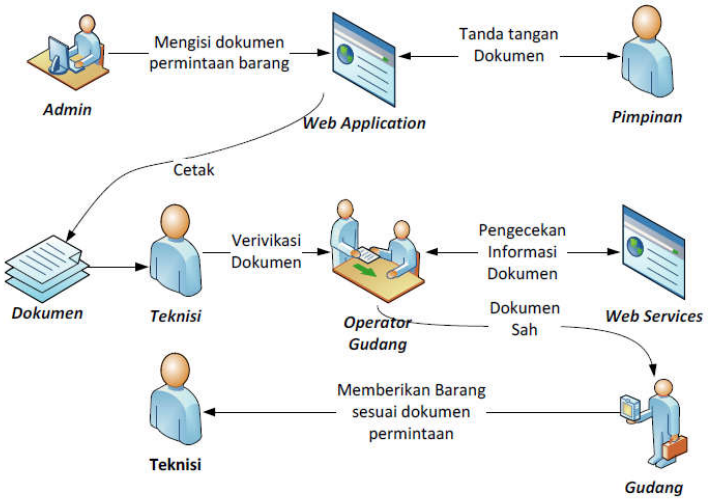
Penelitian ini menggunakan metode penelitian eksperimen. Penelitian eksperimen dapat dikatakan sebagai metode penelitian yang digunakan untuk mencari pengaruh perlakuan tertentu terhadap yang lain dalam kondisi yang terkendalikan (Sugiyono, 2013). Oleh karena itu, penelitian eksperimen erat kaitannya dalam menguji suatu hipotesis dalam rangka mencari pengaruh, hubungan maupun perbedaan terhadap

kelompok yang dikenakan perlakuan. Eksperimen dalam penelitian ini bertujuan untuk menerapkan sitem tanda tangan secara digital yang akurat dan dapat memangkas waktu serta biaya. Dengan metode penelitian ini, informasi dalam QR *Code* yaitu data dokumen dienkripsi dan didekripsi dengan menggunakan algoritma AES, sehingga dokumen tetap terjamin keasliannya dari penyalah gunaan informasi.

a. Proses Tanda Tangan Digital.

1. Teknik perancangan

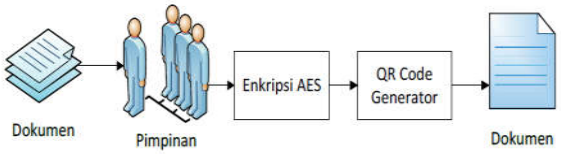
Pada tahap ini akan dilakukan perancangan sistem yang mempresentasikan proses enkripsi dan dekripsi pada *QR Code* dengan menggunakan algoritma *Advaced Eencryption Standard* pada aplikasi tanda tangan digital. Adapun proses dan teknik penerapan tandatangan digital dari aplikasi yang dibangun,yaitu :



Gambar 1. Proses tanda tangan digital.

Proses pertama yaitu *admin* mengisi dokumen permintaan barang kemudian pim- pinan menyetujui dokumen, *admin* akan mencetak dokumen dan memberikan kebagian teknisi, teknisi mengajukan pengambilan barang pada operator gudang dengan menyerahkan dokumen, kemudian operator gudang melakukan proses *secan QR Code* pada dokumen untuk untuk verifikasi keasilian dokumen, jika dokumen permintaan sah maka pihak gudang akan mengambilkan barang sesuai dokumen permintaan.

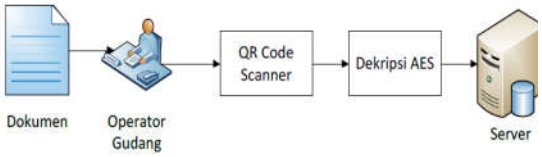
b. Proses *scan Enkripsi QR Code* pada dokumen.



Gambar 2. Proses Enkripsi pada *QR Code*.

Gambar diatas menjelaskan proses pengambilan nomor dokumen dan identitas pimpinan yang akan digunakan sebagai *plaintext*, dilanjutkan dengan proses enkripsi dan pembuatan *QR Code*.

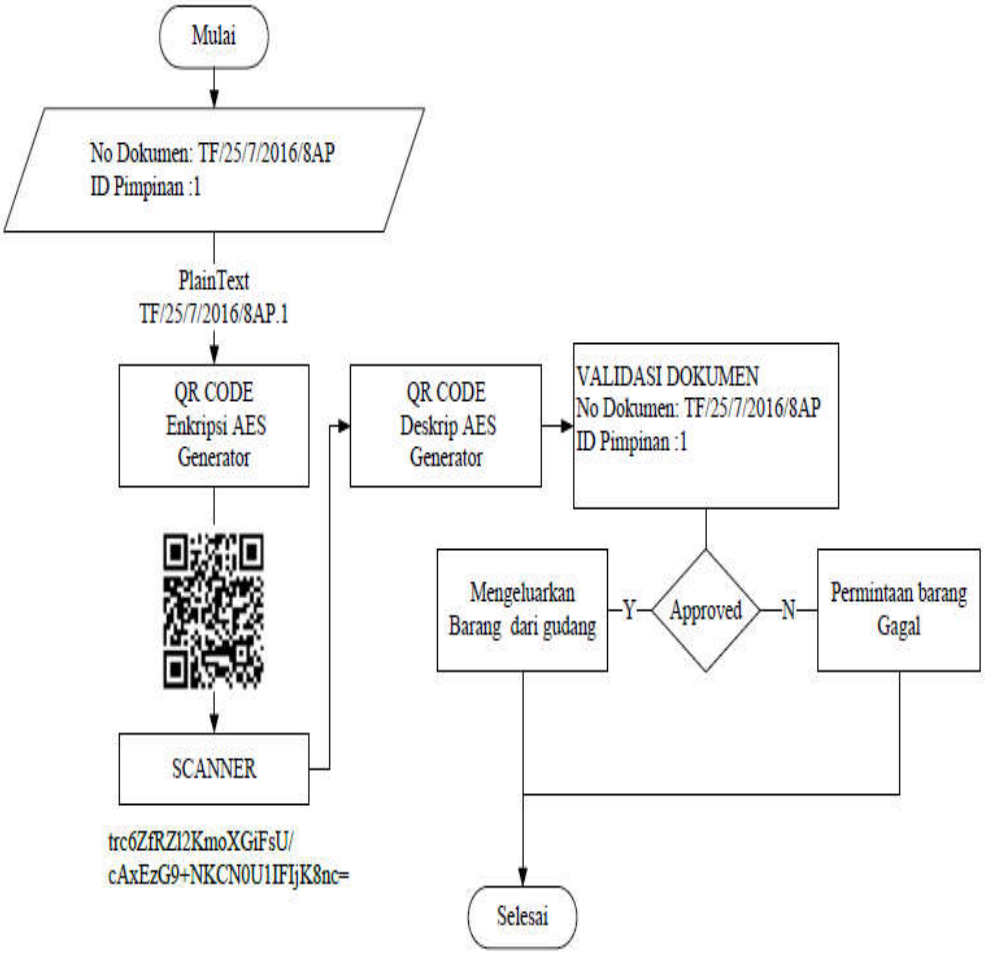
c. Proses Deskripsi dan pembuatan *QR Code*.



Gambar 3. Proses Deskripsi pada *QR Code*.

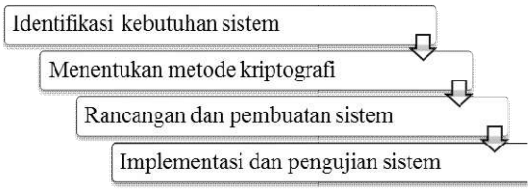
Gambar diatas menjelaskan *QR Code* pada dokumen di scan untuk mengambil informasi *chippertext* dan di dekripsi kembali menjadi *plaintext*, dilanjutkan dengan verivikasi data ke *server*.

d. Penerapan tanda tangan digital.



Gambar 4. Teknik Penerapan Tanda tangan digital.

e. Metode pengembangan sistem. Langkah-langkah yang dilakukan dalam melakukan penelitian ini ditunjukkan pada Gambar 5 dibawah ini:



Gambar 5. Langkah –langkah penelitian.

1. Identifikasi Kebutuhan Sistem, tahapan ini bertujuan untuk melakukan identifikasi kebutuhan perangkat keras dan perangkat lunak yang dibutuhkan dalam penelitian ini.
2. Menentukan Metode Kriptografi, tahapan ini bertujuan untuk menentukan metode kriptografi yang akan digunakan dalam penelitian ini. Adapun metode yang digunakan yaitu kriptografi simetris dengan algoritma *Ad- vanced Encryption Standard(AES)*. Pemilihan algoritma *AES* dikarenakan *AES* memiliki sifat *cipher* yang diharapkan yaitu : tahan menghadapi analisis sandi yang diketahui, fleksibel digunakan dalam berbagai perangkat keras dan lunak, baik digunakan untuk fungsi *hash* karena tidak memiliki *weak*(*semi weak*) *key*, cocok untuk perangkat yang membutuhkan *key agility* yang cepat, dan cocok untuk *stream cipher.*
3. Rancangan dan Pembuatan Sistem, tahapan ini bertujuan untuk melakukan rancangan dan pembuatan aplikasi tanda tangan digital dengan *QR Code* menerapkan algoritma *AES*. Perancangan sistem dengan menggunakan *flowchart*.
4. Implementasi dan Pengujian Sistem, tahapan ini dilakukan implementasi perangkat lunak yang telah dirancang dan pengujian terhadap aplikasi yang dibuat agar sesuai dengan kebutuhan yang telah diajukan, serta pen- gujian validasi dengan menggunakan *Confusion matrix*.

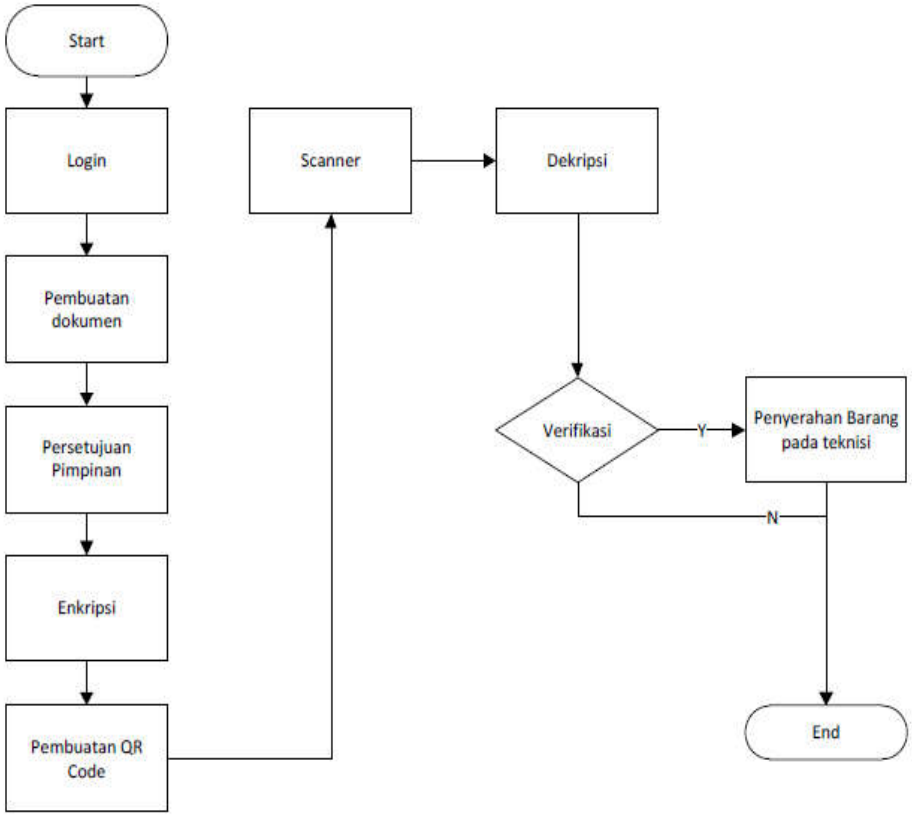
2. *ASP. Net*
ASP.NET merupakan *framework* aplikasi *web* yang dikembangkan dan dipasarkan oleh *Microsoft*. *ASP.NET* memungkinkan pengembang membangun aplikasi *web* yang dinamis dan *web service*. *ASP.NET* dirilis pertama kali pada bulan Januari 2002 dengan versi 1.0 pada *framework .NET* dan merupakan penerus teknologi *Microsoft* yang sebelumnya *ASP*. Dengan *ASP.NET* pengembang dapat menulis kode *ASP.NET* menggunakan bahasa yang didukung oleh *framework .NET* (Hartanto, 2008)
3. *Confusion Matrix*
Metode ini hanya menggunakan tabel matriks terdapat dilampiran jika *dataset* hanya terdiri dari dua kelas, kelas yang satu dianggap sebagai positif dan yang lainnya negatif (Bramer and Max, 2007).
4. Bahasa C#
C# (tanda '#' dibaca "*Sharp*") merupakan bahasa pemrograman baru yang diciptakan *Microsoft* secara khusus sebagai salah satu bahasa baru, C# tdak berevolusi dari bahasa C# versi bukan teknologi .NET. Dengan demikian, C# dapat memaksimalkan kemampuaannya tanpa khawatir dengan masalah kompabilitas dengan versi-versi sebelumnya (Jamaludin, 2006).
5. *SQL Server*
SQL Server mempunyai fitur baru yang bisa membantu seorang *Programmer*, *Database Developer*, atau *database administrator* untuk mengimplementasikan suatu aplikasi baru yang lebih komprehensif. *SQL server* juga mempunyai kelebihan dalam mengelola *database* dan juga dilengkapi dengan kemudahan dalam mengoperasikanya (Nugroho, 2009)

HASIL DAN PEMBAHASAN

Pada penelitian ini di implementasikan dua buah sistem, sistem pertama berbasis *web application*

digunakan oleh *admin* dan pimpinan untuk proses pembuatan dokumen yang diterapkan tantangan digital, sistem kedua berbasis *desktop aplication* digunanakan oleh operator gudang untuk *scan* dokumen. Berikut ini adalah tampilan implementasi:

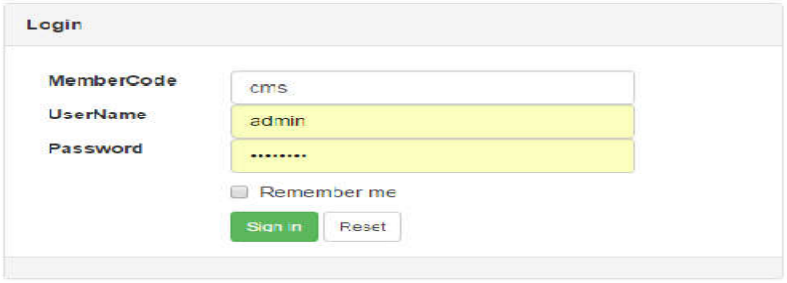
A. Alur Sistem.



Gambar 6. Alur Sistem.

B. ***Web application.***

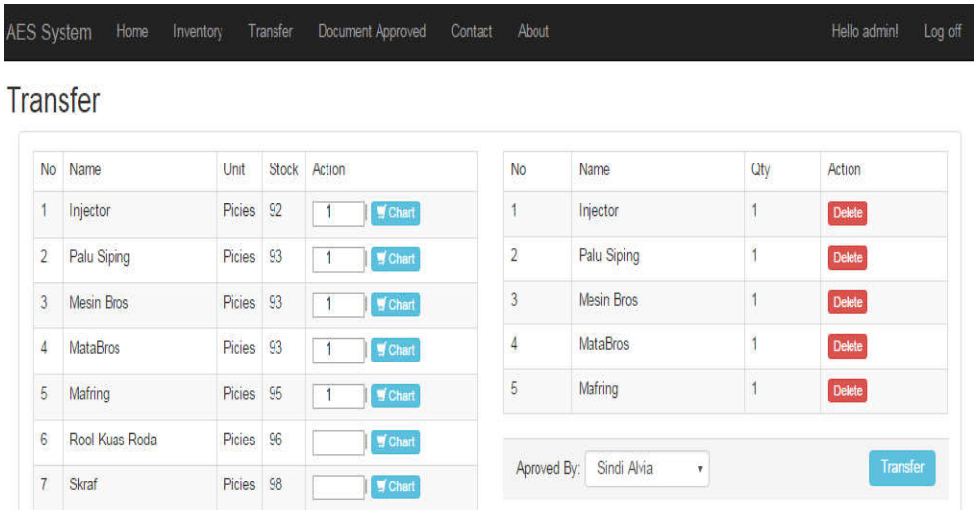
1. *Login*.



Gambar 7. *Login*.

Tampilan halaman *login admin* dan pimpinan seperti gambar di atas.

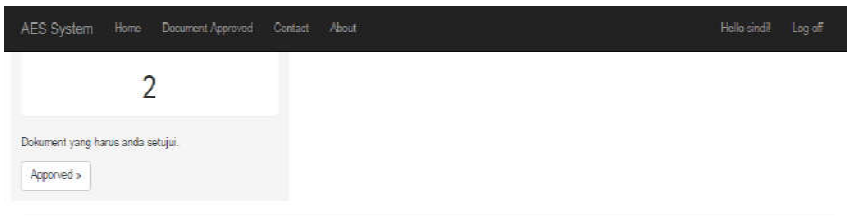
2. *Transfer*.



Gambar 7. *Transfer*.

Admin membuat dokumen permintaan mengisi daftar barang yang dibutuhkan dan di kirim ke pada pimpinan yang bersangkutan. Proses ini dilakukan oleh *admin*, *admin* akan menentukan pimpinan yang bersangkutan untuk sehingga dokumen tersebut dapat di lihat oleh pimpinan yang bersangkutan untuk proses *approved*.

3. Halaman Home Pimpinan.



Gambar 8. Halaman Home Pimpinan.

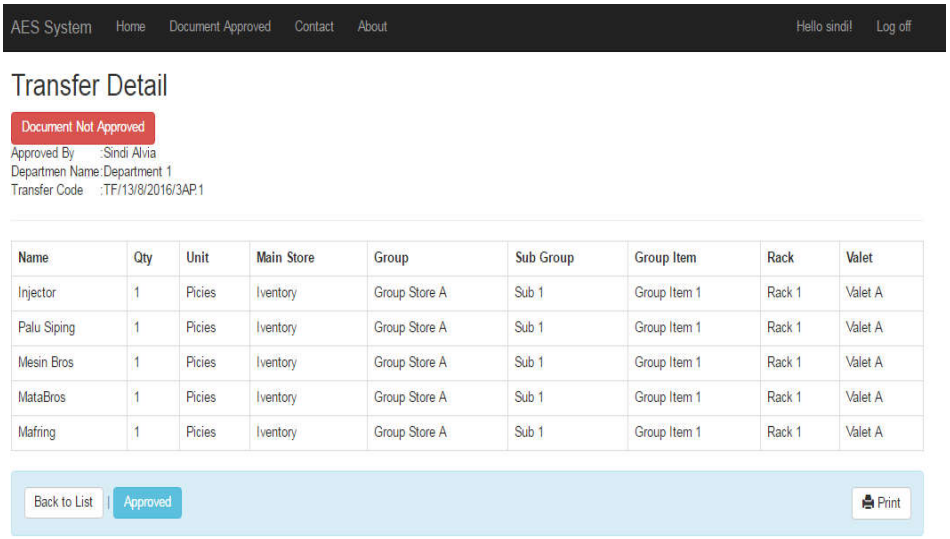
Pimpinan dapat melihat jumlah dokumen yang harus *approved*. Halaman ini login sebagai pimpinan, pimpinan dapat melihat total dokumen yang harus di *approved*.

4. *Transfer department*.

Gambar 9. *Transfer Departement*.

Halaman *Transfer department* menampilkan dokumen permintaan. Halaman ini login sebagai pimpinan, pimpinan dapat melihat list dokumen permintaan dan melihat daftar barang.

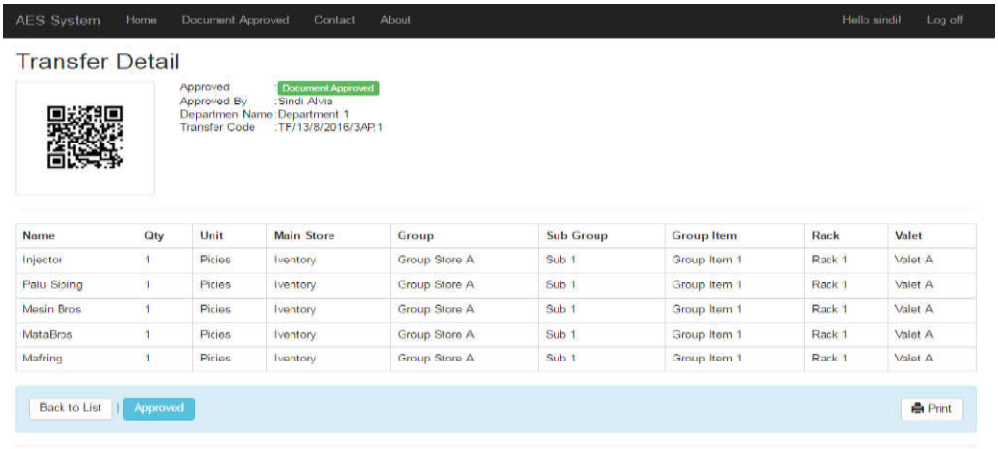
5. *Transfer detail*.
   a) *Transfer detail* sebelum di *approved*.



Gambar 10. *Transfer detail* sebelum *approved*.

Pimpinan melihat daftar barang, jika disetujui makan pimpinan menekan tombol *approved* maka sistem akan otomatis membuat *QR Code* yang terenkripsi.

   b) Transfer *detail* setelah di *approved*



Gambar 11. *Transfer detail* setelah *approved*.

Setelah pimpinan menyetujui, dokumen *QR Code* dokumen tersebut sudah mempunyai tandatangan digital.

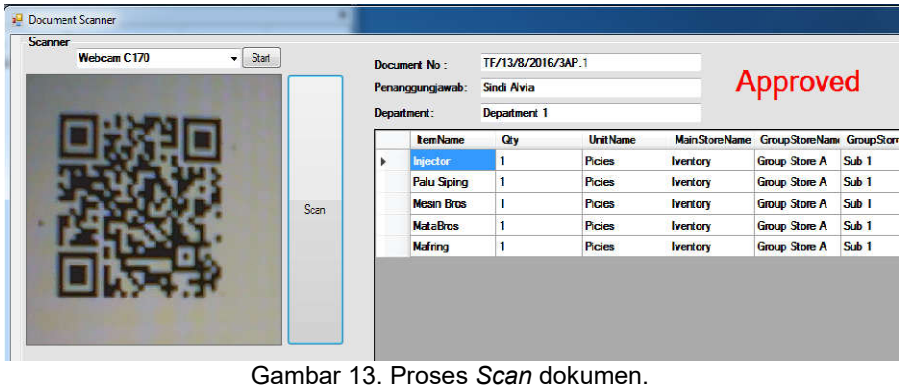
C. Desktop Aplication(Scanner)

1. Tampilan awal aplikasi *scanner*

Gambar 12. Scanner.

Aplikasi ini digunakan oleh operator gudang untuk proses verifikasi dokumen yang sah.

2. Proses *Scan* dokumen.



Gambar 13. Proses *Scan* dokumen.

Dokumen di *scan* dan sistem menunjukan jika dokumen tersebut sah. Sistem mempunyai tingkatan *error* 30% yang sehingga *QR Code* pada dokumen yang mempunyai kerusakan 30% sistem menunjukan informasi kepada user bahwa dokumen tersebut tidak sah.

KESIMPULAN

Kesimpulan dari penelitian ini dapat diuraikan sebagai berikut : Berdasarkan penelitian yang telah di lakukan maka dapat di ambil kesimpulan bahwa penerapan *QR Code* menggunakan algoritma *Advanced Encryption Standard* sebagai tanda tangan digital dapat berfungsi sebagai otentikasi tanda tangan pimpinan serta verivikasi dokumen pengambilan barang yang sah. dari penelitian ini akurasi klasifikasi *QR Code* dengan menggunakan *naïve bayes classifier* sebesar 90% dengan *precision positif* sebesar 80% dan *precision* negatif sebesar 100%.

DAFTAR PUSTAKA

Bramer, Max. (2007). *Principles of Data Mining*. London: Springer. ISBN-10: 1-84628-765-0, ISBN-13: 978-1-84628-765-7.

Hartanto, B. 2008, *Memahami Visual C#.NET secara mudah*, Penerbit ANDI, Yogyakarta

Jamaludin, ST. 2006, *Belajar sendiri .net dengan visual C# 2005*, Penerbit ANDI, Yogyakarta.

Nugroho, A. (2009). *Menguasai T-SQL QUERY + Programming SQL Server 2008*, C.V. Andi Offset, Yogyakarta

Sugiyono. 2013*, Metode Penelitian Pendidikan (Pendekatan Kuantitatif, Kualitatif, dan R&D)*. Bandung : Alfabeta.