

Rancang Bangun *E-Commerce* Untuk Meningkatkan Penjualan Petani Ikan Menggunakan Algoritma *Rivest Shamir Adleman* (Studi Kasus : Desa Koto Tibun)

Lucky Lhaura Van FC
Program studi Teknik Informatika
Fakultas Ilmu Komputer Universitas Lancang Kuning
Email : lucky@unilak.ac.id

Abstrack - Several problems experienced by fish farmers when selling and marketing fish such as; fish are sold to collectors at a price that is set by the collectors, and fish in the collectors are sold at a price that is much more expensive than the price that has been set to the fish farmers. To avoid selling to collectors and to market medium freshwater then it is needed ane-commerceapplication that can simplify the transaction, especially through mobile devices like smartphone. This study aims to provide a service that can help fish farmers to sell and market their fish. Modeling used in the development of this application is waterfallmodeling anduses UML(UnifiedModelingLanguage)as a tool for modeling system. This application uses a RSA (Rivest Shamir Adleman) algorithm as security to encrypt customers' data such as customer's passwords, address and mobile phone number.

Keywords: E-Commerce, Fish, Rivest Shamir Adleman, Android

Intisari – Berbagai masalah yang dialami oleh petani pada saat menjual ikan dan memasarkan ikan seperti, ikan di jual kepada pengepul dengan harga yang di tetapkan pengepul, ikan yang sudah melewati pengepu ldijual dengan harga yang jauh lebih mahal dari pada harga yang sudah di tetapkan kepada petani ikan. Untuk menghindari penjualan ke pengepul dan sebagai media pemasaran air tawar maka di butuhkannya suatu aplikasi *e-commerce* yang dapat mempermudah dalam bertransaksi khususnya melalui media perangkat bergerak seperti *smartphone*. Penelitianini bertujuan untuk menyediakan layanan yang dapat membantu petani ikan menjual dan memasarkan ikan. Pemodelan yang digunakan dalam pengembangan aplikasi ini adalah pemodelan waterfall dan menggunakan UML (*Unified Modeling Language*) sebagai alat bantu pemodelan sistem. Aplikasi ini menggunakan algoritma RSA (*Rivest Shamir Adleman*) sebagai sekuriti untuk mengenkripsi data pelanggan seperti password pelanggan, alamat pelanggan dan nomor handphone pelanggan.

Kata Kunci : E-Commerce, Ikan, Rivest Shamir Adleman, Android

I. PENDAHULUAN

Indonesia memiliki sumber daya perikanan yang sangat potensial, baik diwilayah perairan tawar (darat), pantai maupun perairan laut.Potensi sumber dayaperairan tawar meliputi keanekaragaman jenis ikan dan lahan perikanan.Budidaya perikanan air tawar di Riau yang didominasi oleh perikanan budidayakolam dan keramba dengan ikan jenis patin dan nila sebagai produk unggulan.Potensi ikan semakin besar

ditopang oleh luasnya lahan perikanan budidaya airtawar di Riau, berupa sungai, waduk untuk budidaya keramba dan lahan pembuatan tambak.

Salah satu daerah yang ada di Provinsi Riau tepatnya Desa Koto Tibun Kecamatan Kampar Kabupaten Kampar sebagian masyarakatnya memiliki usaha budidaya ikan air tawar, petani ikan menjual ikannya kepada pengepul, harga ikan di tetapkan oleh pengepul, harga ikan yang telah melewati pengepul jauh lebih mahal dari pada harga yang di buat oleh petani ikan,

pengepul melakukan pembayaran kepada petani ikan secara bertahap. Untuk menghindari penjualan ke pengepul dan sebagai media pemasaran air tawar maka di butuhkan suatu aplikasi yang dapat mempermudah dalam bertransaksi khususnya melalui media perangkat bergerak seperti *smarphone* atau *tablet*.

Pada sebuah aplikasi *mobile* atau *website* yang biasanya terdapat *form* yang dapat diisi oleh member sehingga bisa berinteraksi secara penuh dengan aplikasi *mobile* atau *website* tersebut. Dalam pengisian *form* dalam sebuah aplikasi *mobile* atau *website*, biasanya terdapat isian-isian yang mengharuskan kita untuk menginputkan data pribadi secara lengkap yang akan di simpan di *server*. Selain itu kita biasanya diharuskan untuk menjadi member dari dari aplikasi *mobile* atau *website* tersebut dan sebelumnya kita harus membuat *account* dengan membuat *email*, *password* dan data pribadi yang aka dibutuhkan ketika kita masuk atau *login* ke aplikasi *mobile* atau *website* itu. Untuk menjaga keamanan dari *email*, *username* dan data pribadi, biasanya digunakan teknik enkripsi agar kerahasiaan data tersebut terjamin. Jelaslah bahwa teknik enkripsi sangat penting dalam pengamanan data.

Ada beberapa algoritma enkripsi yang biasa digunakan seperti DES, Triple DES, Blowfish, IDEA, RSA (Rivest-Shamir-Adleman) dan sebagainya. Khusus untuk RSA merupakan algoritma pertama yang cocok untuk *digital signature* seperti halnya enkripsi, dan salah satu yang paling maju dalam bidang kriptografi *public key*. RSA masih digunakan secara luas dalam protokol *electroniccommerce*, dan dipercaya dalam mengamankan dengan menggunakan kunci yang cukup panjang. Algoritma-algoritma tersebut begitu rumit dan sulit dimengerti dengan dalih “faktor keamanan”, katanya semakin sulit algoritma untuk dimengerti, maka semakin aman. Namun bagi para pengguna mereka tidak memikirkan seberapa sulit algoritma dan aplikasinya, yang mereka

inginkan hanyalah menjaga kerahasiaan data.

Dengan keunggulan yang dimiliki android maka muncul gagasan untuk membuat *e-commerce* penjualan ikan air tawar berbasis android guna menyelesaikan masalah, maka penulis berinisiatif untuk merancang dan membuat media yang berguna untuk melakukan transaksi pemesanan dan penjualan ikan serta dapat membantu memenuhi kebutuhan.

Masalah yang dirumuskan pada penelitian ini adalah sebagai berikut:

Pertama, Bagaimana merancang dan membuat aplikasi *e-commerce*, Kedua Bagaimana menerapkan algoritma Rivest Shamir Adleman pada aplikasi *e-commerce*, Ketiga Bagaimana petani ikan menghindari menjual ikan kepada pengepul dengan harga murah. Keempat Bagaimana pemasaran ikan air tawar lebih di kenal oleh masyarakat.

Setelah dilakukan penelitian ke desa koto tibun negeri rumbio kab. Kampar, penulis menemukan beberapa permasalahan yang harus segera dibenahi diantaranya: Penjualan ikan yang berjalan sangat merugikan petani ikan karena adanya peran pengepul yang meletakkan harga ikan dibawah standar dan sulit memasarkan ikan sehingga pengelola kesulitan mengembangkan pangsa pasarkeluar dari desa koto tibun.

Berkaitan dengan hal tersebut, maka sangat diperlukan membangun aplikasi *e-commerce* untuk layanan jual beli ikan sekaligus menjadi sarana promosi sehingga dapat memberikan informasi kepada masyarakat luas penghasil ikan oleh petani ikan di desa koto tibun.

II. SIGNIFIKASI STUDI

A. Studi Literatur

Seema Verma dan Deepak garg, *An Improved RSA Variant*, [1] dimana Karena RSA adalah yang paling populer dan banyak digunakan dalam *e-commerce*, ada kebutuhan untuk membuatnya lebih dan lebih efisien. Salah satu varian RSA, yaitu Dual RSA, dirancang untuk mengurangi

konsumsi memori untuk dua contoh RSA. Berdasarkan Dual RSA Small d , skema baru dirancang sedemikian rupa sehingga waktu enkripsi online menjadi hampir dapat diabaikan karena memiliki kinerja dekripsi yang sama seperti pada Dual RSA kecil d . Skema ini diimplementasikan untuk mencerminkan hasil teoritis. Skema yang dihasilkan efisien dalam enkripsi, kinerja dekripsi dan konsumsi memori. Oleh karena itu skema ini cocok untuk digunakan di lingkungan terbatas sumber daya. Skema juga menunjukkan properti keamanan semantik.

Penelitian selanjutnya dilakukan oleh Atmoko Nugroho, April Firman Daru dan Whisnumurti Adhiwibowo dari Fakultas Teknologi Informasi dan Komunikasi, Universitas Semarang pada tahun 2014, yang berjudul "Pengembangan Pemasaran Online Usaha Kerajinan Enceng Gondok dan Pandan di Desa Lopait Kecamatan Tuntang Kabupaten Semarang". Menurut Atmoko Nugroho, April Firman Daru dan Whisnumurti Adhiwibowo (2014) model pemasaran konvensional mensyaratkan banyak biaya dengan segala keterbatasannya. Dengan berkembangnya teknologi informasi dan mudahnya akses internet membawa dampak semakin mudahnya mengembangkankan pemasaran online. Pemanfaatan internet untuk memasarkan suatu produk memiliki jangkauan lebih luas dibanding memasarkan secara konvensional. Konsumen dapat melihat dan mempelajari produk tanpa dibatasi ruang dan waktu, selama akses internet ada. *Web commerce* yang dibuat untuk aryani art dan koen gallery menjadi sarana pemasaran yang efektif untuk menjangkau konsumen yang lebih luas diberbagai belahan dunia. Melalui cara ini, aryani art dan koen gallery memasuki pemasaran tanpa batas.

Penelitian lain juga dilakukan oleh Melinda Novia, rostianingsih dan setiabudi, dimana penelitian ini merancang dan membuat e commerce untuk jackpot pancing, yang gunanya e commerce ini dapat meningkatkan sistem penjualan yang

ada, mulai dari safety stok sampai mempermudah konsumen dalam memilih milih produk yang dijual pada jackpot pancing ini.

Penelitian lain oleh J.Nwoye, [4] membahas E-commerce telah menghadirkan cara baru dalam melakukan transaksi di seluruh dunia menggunakan internet. Keberhasilan e-commerce sangat tergantung pada bagaimana teknologi informasinya digunakan. Selama bertahun-tahun, tingkat di mana informasi sensitif e-commerce dikirim melalui internet dan jaringan telah meningkat secara drastis. Karena alasan inilah setiap perusahaan ingin memastikan bahwa informasi e-niaga dijamin. Ada kebutuhan untuk informasi e-commerce yang dikirimkan melalui internet dan jaringan komputer untuk dilindungi. Ada pertumbuhan substansial di bidang penipuan kartu kredit dan pencurian identitas karena internet adalah jaringan publik dengan ribuan juta pengguna. Di antara para pengguna adalah cracker atau peretas yang melakukan penipuan kartu kredit dan pencurian identitas dengan berbagai cara yang difasilitasi oleh keamanan internet yang buruk; kekhawatiran tentang pertukaran uang dengan aman dan nyaman melalui internet meningkat. Kritikan, bahaya, dan kepentingan prioritas yang lebih tinggi dari setiap transfer uang e-commerce menjadikannya sebuah area penelitian yang menarik di bidang ilmu komputer modern dan informatika. Industri e-commerce perlahan-lahan mengatasi masalah keamanan di jaringan internal mereka tetapi perlindungan keamanan bagi konsumen masih dalam masa pertumbuhan, sehingga menjadi penghalang bagi pengembangan e-commerce. Ada kebutuhan yang berkembang untuk solusi teknologi untuk informasi transaksi e-niaga yang aman secara global dengan menggunakan teknologi keamanan data yang tepat. Solusi teknologi yang diusulkan untuk memecahkan masalah keamanan ini adalah cryptosystem RSA. Makalah penelitian ini

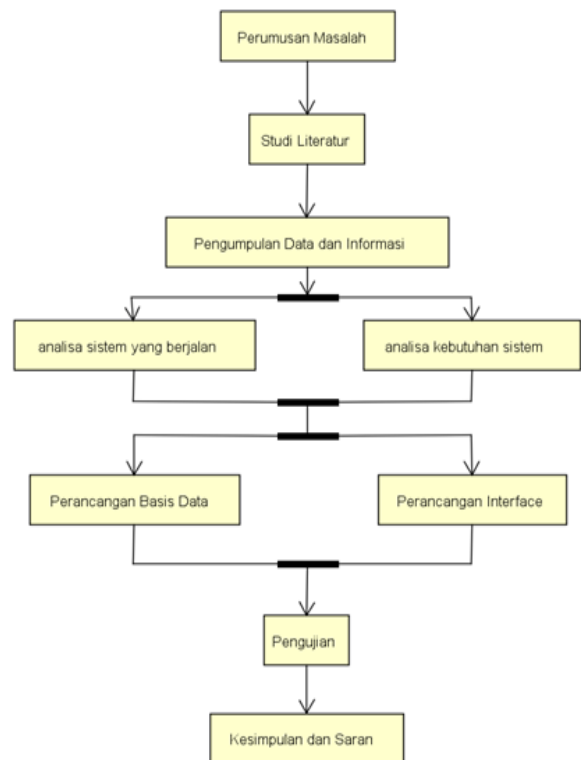
berfokus pada mengamankan informasi e-commerce yang dikirim melalui jaringan komputer dan internet menggunakan kriptografi RSA. Ini menjelaskan penerapan algoritma RSA dan menunjukkan bahwa keamanan e-commerce yang didukung dengan kriptografi RSA sangat penting dalam transaksi e-niaga.

Penelitian selanjutnya dilakukan oleh Sandy Kosasi dari STMIK pada tahun 2015, yang berjudul “Perancangan Sistem E-Commerce Untuk Memperluas Pasar Produk Oleh-Oleh Khas Pontianak”. Menurut Sandy Kosasi (2015) Perancangan sistem *E-Commerce* khusus produk oleh-oleh khas Kota Pontianak memiliki fasilitas untuk menyimpan data pribadi member (anggota) dengan dilengkapi dengan *username* dan *password* untuk mengantisipasi penyalahgunaan oleh orang-orang yang tidak bertanggung-jawab. Sistem *E-Commerce* ini juga menyediakan fasilitas pembayaran melalui transfer bank dan *Cash On Delivery*.

Penelitian lain yang menunjukkan peningkatan penjualan karena *e-commerce* adalah menurut lhaura [7] yaitu Semakin berkualitas pelayanan *e-commerce* yang disediakan para pengelola situs belanja fashion online, maka semakin tinggi tingkat keputusan konsumen untuk membeli fashion secara online. Rendahnya persepsi resiko dan tingginya kualitas pelayanan elektronik secara bersamaan akan mampu meningkatkan keputusan konsumen untuk membeli fashion secara online.

B. Metode Penelitian

Penelitian ini menggunakan Pemodelan *Waterfall*. Model ini melakukan pendekatan secara sistematis dan urut mulai dari level kebutuhan sitem lalu menuju ketahap analisis, desain, *coding*, *testing*, dan *maintenance*. Disebut *waterfall* karena tahap demi tahap yang dilalui harus menunggu selesainya tahap sebelumnya dan berjalan berurutan, sebagai contoh tahap coding, harus menunggu tahap desain selesai. Adapun tahap penelitian seperti gambar 1 dibawah ini :



Gambar 1. Tahapan Penelitian

Penelitian ini juga menggunakan algoritma-RSA sebagai sekuriti untuk membuat tulisan rahasia yang aman dari campur tangan pihak ketiga atau pihak yang tidak diharapkan. Algoritma atau hitungan kriptografi dapat disebut juga *chipper* yaitu hitungan matematik yang digunakan untuk membuat suatu enkripsi maupun dekripsinya.

Terdapat 3 algoritma pada system kriptografi-RSA, yaitu algoritma pembangkit kunci, algoritma enkripsi, dan algoritma deskripsi.

1. Pembangkitkunci RSA

Untuk menggunakan RSA terlebih dahulu pendekripsi (Bob) membangkitkan sepasang kunci yaitu kunci public dan kunci privat. Bangkitkan bilangan prima besar p dan q.

$$\begin{aligned}
 n &= p \times q \\
 \phi(n) &= (p - 1) \times (q - 1) \\
 e &\in \mathbb{Z}_{\phi(n)} \text{ dengan } \text{gcd}(e, \phi(n)) = 1 \quad (1) \\
 d &= e^{-1} \text{ pada } \mathbb{Z}_{\phi(n)} \\
 K_{\text{publik}} &= (e, n), K_{\text{privat}} = d
 \end{aligned}$$

2. *Enkripsi*

Setelah kunci public K_{publik} dibangkitkan oleh pendekripsi (Bob) maka sembarang orang dapat menggunakan kunci publik Bob untuk mengirim teks sandi ke Bob.

Input: $K_{publik} = (e,n), P \in Z_n$
 Output : $C \in Z_n$ (2)
 $C = P^e \text{ mod } n$

3. *Deskripsi*

Jika Bob mendapatkan teks sandi yang di enkripsi dengan kunci publik Bob, maka Bob- dapat menggunakan kunci privatnya untuk mengembalikan teks asli. Sama seperti enkripsi, algoritma dekripsi RSA merupakan fungsi eksponensial modular n dengan menggunakan kunci privat.

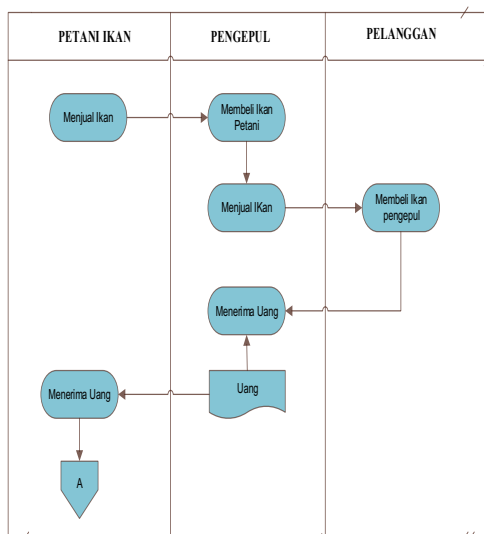
Input : $K_{privat} = d, K_{publik} = (e,n), P \in Z_n$
 Output : $P \in Z_n$ (3)
 $P = C^d \text{ mod } n$

III. HASIL DAN PEMBAHASAN

Setelah merancang menggunakan metode waterfall mulai dari tahap kebutuhan sistem maka akan sampai pada tahap evaluasi.

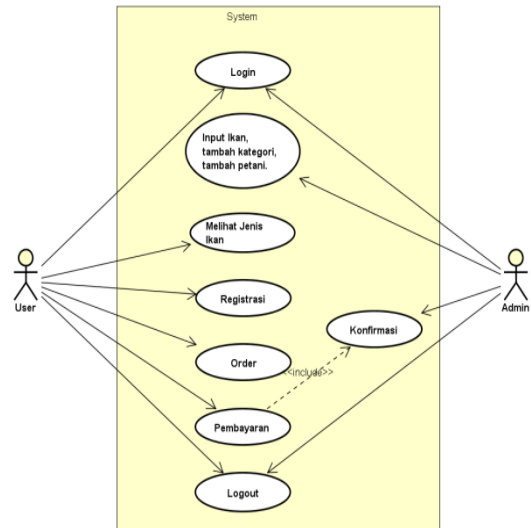
A. *Evaluasi*

Sebelum tahap evaluasi, peneliti menganalisa sistem yang sedang berjalan, seperti pada gambar 2 dibawah ini :



Gambar 2. Aliran Sistem Informasi

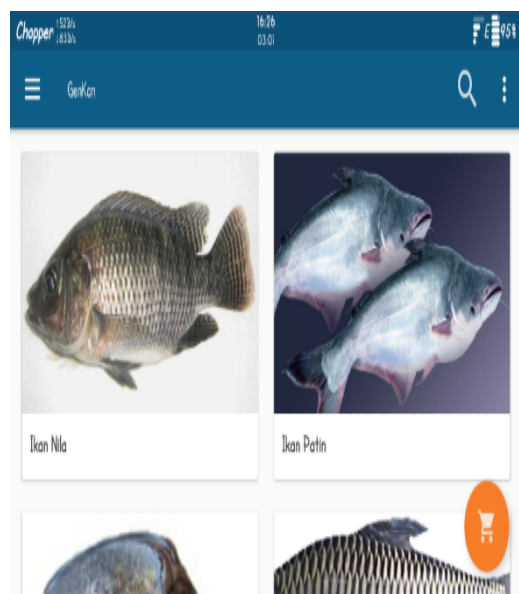
Setelah dilakukan evaluasi terhadap analisa yang sedang berjalan maka dibuat Rancangan sistem use case nya sebagaimana gambar 3 berikut :



Gambar 3. Use Case Diagram

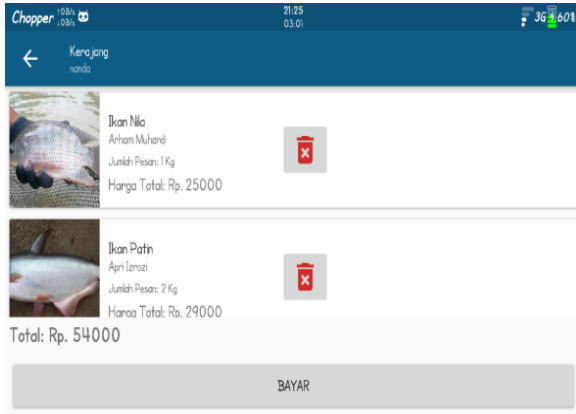
B. *Hasil*

Desain tampilan menu utama merupakan rancangan *interface* yang pertama kali muncul ketika buka aplikasi *e-commerce*. Pada menu utama ini *user* dapat melihat dagangan ikan berdasarkan kategori.



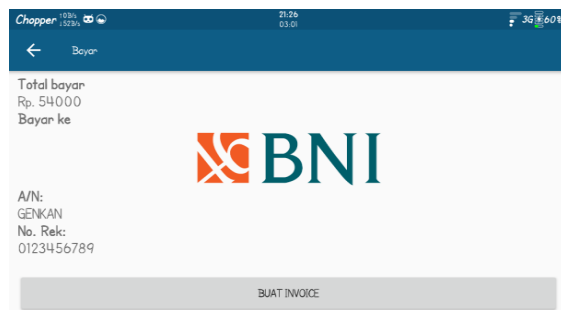
Gambar 4. Menu Utama User

Tetampilan keranjang belanja pelanggan, ketika pelanggan berbelanja dengan jenis ikan yang berbeda maka akan masuk ke keranjang belanja.



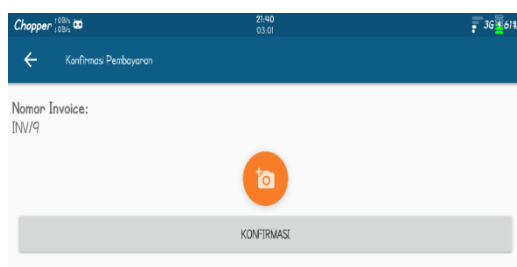
Gambar 5. Keranjang Belanja

Kemudian tampilan untuk membayar belanja, pelanggan akan di minta melakukan tranfer uang ke rekening yang sudah di ditetapkan, dan pelanggan akan melihat dan dapat mengeprint *invoice* (dokumen tagihan) dari hasil belanja.



Gambar 6. Total bayar dan rekening transfer

Selanjutnya Merupakan tampilan untuk mengkonfirmasi pembayaran yang sudah di lakukan oleh pelanggan dengan mengupload foto bukti pembayaran.

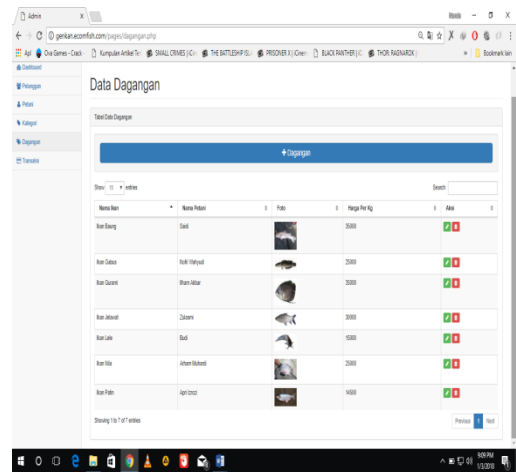


Gambar 7. Konfirmasi Pembayaran

C. Pembahasan

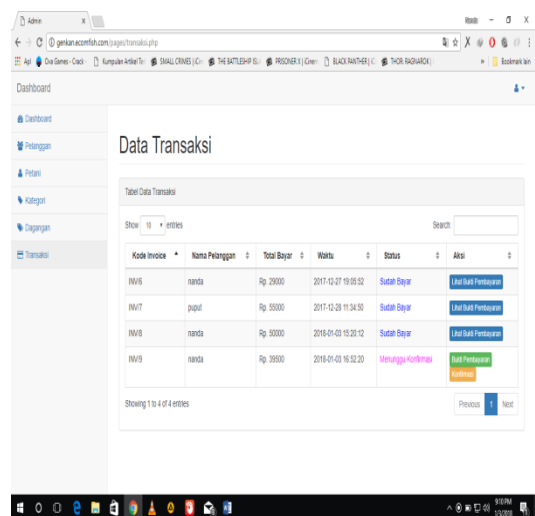
Setelah dilaksanakan evaluasi terhadap sistem yang dibangun ,dimana dimulai dari menu login, katalog ikan, pembayaran, maka ditemukan suatu pembahasan yang mana sistem yang dibangun menambahkan menampilkan stok ikan yang tersedia untuk di jual.

Dibawah ini Merupakan Tampilan dagangan ikan yang jual yang tujuan tampilan ini mempermudah petani dalam melengkapi data ikan yang ada dan memudahkan pembeli melihat ikan yang dibutuhkan untuk dibeli.



Gambar 8 Katalog Ikan

Pada Gambar dibawah merupakan tampilan data transaksi pelanggan, dan menu untuk melakukan konfirmasi pembayaran.



Gambar 8. Transaksi Pelanggan

Pada Gambar diatas, setelah dilakukan transaksi pembelian maka penjual dan pembeli bisa mencetak bukti transaksi.

IV. KESIMPULAN

1. Dengan menggunakan aplikasi *e-commerce* ini, jangkauan penjualan menjadi lebih luas dan aplikasi ini dapat digunakan oleh pengguna smartphone.
2. Dengan adanya aplikasi ini pelanggan akan mengetahui harga dari berbagai jenis ikan yang di jual.

Keterbatasan sistem adalah:

1. Secepatnya harus meningkatkan pelayanan pada unsur yang belum memenuhi harapan pelanggan.
2. Sebaiknya melakukan penelitian secara berkala untuk mengetahui kepuasan dari *e-commerce* terhadap kualitas pelayanan yang diberikan dan hasilnya perlu dievaluasi serta ditindak lanjuti.

REFERENSI

- [1] Seema Verma dan Deepak garg .2014,An Improved RSA Variant .
- [2] Melinda Novia,rostianingsih dan setiabudi.2015.Perancangan dan Pembuatan E-commerce pada UD.Jackpot Pancing
- [3] Nugroho, Atmoko, April Firman Daru, Whisnumurti Adhiwibowo. 2014. Pengembangan Pemasaran Online Usaha Kerajinan Enceng Gondok Dan Pandan Di Desa Lopait Kecamatan Tuntang Kabupaten Semarang. Jurnal Transformatika, Volume 12, No. 1.
- [4] J.Nwoye Chinedu.Design and Development of an E-Commerce Security Using RSA Cryptosystem.2015
- [5] Jogiyanto. 2005. Analisis dan Desain Sistem.Yogyakarta : Andi
- [6] Kosasi, Sandy. 2015. Perancangan Sistem E-Commerce untuk Memperluas Pasar Produk Oleh-Oleh Khas Pontianak.Snastia, ISSN 1979-3960
- [7] Van FC, Lucky Lhaura, and Lisnawita Lisnawita. "Pengaruh persepsi resiko dan kualitas e-commerce terhadap keputusan konsumen membeli fashion online." Digital Zone: Jurnal Teknologi Informasi dan Komunikasi 8.2 (2017): 185-195.
- [8] Sadikin, Rifki. 2012. Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java. Yogyakarta : Andi
- [9] Safaat, Nazruddin H. 2012. ANDROID Pemograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android. Bandung : Informatika
- [10] Sholih, Fachrul Barry. 2014. Aplikasi Penjualan Batik Berbasis Android (Studi Kasus di Batik Puspa Kencana, Laweyan, Solo).Surakarta :Universitas Muhammadiyah.
- [11] Sutabri, Tata. 2012. Konsep Sistem Informasi. Yogyakarta: Andi
- [12] Udin, Muhammad Amir. 2014. Perancangan dan Implementasi E-Commerce untuk Meningkatkan Penjualan Produk Herbal Pada Toko La Roiba.Semarang : Universitas Dian Nuswantoro.
- [13] Wijaya, Hendi, Wellia Shinta Sari. 2015. Rancang Bangun Mobile Commerce Berbasis Android Pada Toko Duta Buku Semarang.Techno.COM, Vol. 14, No. 2.