ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

STUDI LITERATURE KEAMANAN VIRTUAL CREDIT CARD DALAM TRANSAKSI

Alana Nabihah Thufailah[1)], **Faraz Nurdini**[2)], **Nur Aini Rakhmawati**[3)]

[1), 2)] *S1 Sistem Informasi, Institut Teknologi Sepuluh Nopember*
Email : alanathufailah.205026@mhs.its.ac.id[1)], f.nurdini04@gmail.com[2)], nur.aini@is.its.ac.id[3)]

ABSTRACT

The use of virtual credit cards is increasing as technology develops. Not a few virtual credit card users use the virtual card to make purchase transactions, such as online transactions at merchants or e-commerce. However, the use of virtual credit cards is still at risk of theft of personal data and phishing. This analysis aims to infer the fundamental algorithms and theories that support the creation of virtual credit cards and how their security systems are formed by literature study research methods to compare the results of virtual credit card research with others, then conclude the advantages and disadvantages of each proposed method. Our analysis concluded that the use of virtual credit cards is often used as a one-time use, with each number using an algorithm that has billing and merchant information.

Keywords : *VCC, Security, Card*

ABSTRAK

Penggunaan virtual credit card semakin banyak selagi berkembangnya teknologi. Tidak sedikit pengguna virtual credit card menggunakan kartu virtual tersebut untuk melakukan transaksi pembelian, seperti transaksi online pada merchant atau e-commerce. Namun penggunaan virtual credit card masih beresiko dengan adanya pencurian data pribadi dan phising. Analisis ini bertujuan untuk menyimpulkan algoritma dan teori mendasar yang menunjang pembuatan virtual credit card dan bagaimana sistem keamanannya terbentuk dengan metode penelitian studi literatur untuk membandingkan hasil penelitian virtual credit card dengan lainnya, lalu menyimpulkan kelebihan dan kekurangan dari tiap metode yang diusulkan. Aanalisis kami menyimpulkan bahwa penggunaan virtual credit card kerap digunakan sebagai one-time use atau penggunaan sekali pakai, dengan masing-masing angka menggunakan algoritma yang memiliki informasi billing dan merchant.

Kata Kunci : *VCC, Security, Card*

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

1. Pendahuluan

Melakukan transaksi bisnis tanpa menggunakan uang tunai sudah menjadi hal yang umum ditemui pada era modern ini. Dengan berkembangnya teknologi secara pesat dari zaman ke zaman, tentunya kegiatan komersial pun akan mengikuti pula perkembangan yang serupa. Sebelum terjadi kemajuan teknologi yang pesat dalam bidang ekonomi, masyarakat pada umumnya menggunakan pembayaran menggunakan koin dan uang kertas sebagai opsi utama dalam transaksi. Pada tahun 1952, diciptakanlah kartu kredit resmi bank pertama oleh bank komersial pertama di Amerika yaitu *Franklin National Bank* **(Douglas, 2018)**.

Kartu kredit sendiri merupakan alternatif pembayaran menggunakan kartu dimana seseorang melakukan transaksi yang biayanya akan ditanggung terlebih dahulu oleh penerbit kartu tersebut, kemudian sang konsumen harus membayar kembali penerbit kartu dengan syarat dan ketentuan yang telah ditetapkan sebelumnya. Biasanya, kartu kredit mampu digunakan dalam pembayaran di toko-toko tertentu yang memiliki *electronic data capture* (EDC). EDC adalah sebuah mesin khusus dimana kartu akan digesek, ditempelkan, atau dimasukkan ke dalam celah spesifik untuk membaca chip kartu, kemudian pelanggan harus memasukkan pin rahasia rekening mereka sebelum pembayaran ditagihkan ke bank penerbit kartu. Ketika era digital timbul dan perlahan tumbuh dalam ranah ekonomi, muncullah pasar digital atau *electronic commercial* yang kerap juga dikenal sebagai *e-commerce.*

E-commerce di dunia dimulai pada tahun 1970-an, dimana perusahaan-perusahaan ingin melakukan transaksi melalui komputer dengan sistem yang saat itu dinamakan *electronic data interchange* (EDI). Cara transaksi tanpa tunai dan kertas ini terus berkembang perlahan-lahan hingga pada akhirnya, *e-commerce* bisa meranah ke internet dan mampu diakses oleh khalayak luas pada tahun 1990 **(Hermogeno, 2019)**. Pada era digital ini, jangkauan dari *e-commerce* sudah meluas ke banyak sektor penting terutama saat terjadinya pandemi Corona Virus Disease 2019 (COVID-19) pada 2019 lalu. Sebagai dampaknya, masyarakat terpaksa untuk melakukan kegiatan utamanya secara online, termasuk berbelanja guna memenuhi kebutuhan sehari-hari **(Permana, Reyhan, Raffli, & Rakhmawati, 2021)**. Mengingat *e-commerce* sendiri merupakan pusat perbelanjaan berbasis digital, membayar melalui tunai justru merupakan hal yang tidak terlalu efektif dikarenakan terdapat beberapa resiko saat proses pembayaran dilakukan, seperti pelanggan kabur dengan barang tanpa membayar produk yang dibeli, uang yang dititipkan kurir untuk membayar dibawa kabur, atau kendala transportasi mahal hanya untuk menyerahkan uang secara fisik ke penjual. Maka dari itu, untuk menanggulangi berbagai permasalahan yang muncul, terbitlah kartu kredit sebagai salah satu opsi pembayaran yang dapat digunakan dalam belanja secara online. Pembayaran menggunakan kartu kredit biasanya dilakukan dengan cara memasukkan informasi yang tergolong sensitif seperti nama pemegang kartu, nomor kartu kredit yang digunakan, masa berlaku kartu, dan kode verifikasi kartu (CVV) sebelum tagihan bisa diberikan.

Karena transaksi menggunakan kartu kredit untuk berbelanja sudah tidak jarang lagi, tidak mengherankan jika terdapat pelanggan yang lengah akan keamanan data akan asal mengisi informasi kartu kredit mereka tanpa benar-benar memastikan dimana mereka memasukkannya. Hal ini menyebabkan terjadinya banyak kejahatan pencurian data pribadi yang berisi data-data kartu yang nantinya dijual di internet, kemudian dibeli dan digunakan oleh penipu agar bebas dari tagihan belanja mereka serta merugikan banyak pihak, terutama pemilik kartu, penerbit kartu, dan penjual dalam transaksi yang sedang berjalan **(Hendarsyah, 2020)**.

Untuk menanggulangi resiko dari tercurinya data pribadi pemegang kartu kredit, muncullah sebuah solusi dimana nomor kartu kredit dan kode verifikasi kartu dapat dihasilkan dari urutan nomor acak online sebelum diberikan oleh bank penerbit kepada sang pemohon kartu. Setelah mendapat nomor acak tersebut, kartu kemudian dapat digunakan dalam jangka waktu tertentu dan terbatas hanya untuk beberapa transaksi saja. Sistem ini dinamakan sebagai *virtual credit card* (VCC) **(Kumar, Kumar, Raj, & Shah, 2018)**. Cara VCC diciptakan juga tidak sama bagi setiap penyedia layanan pembuatan, masing-masing memiliki algoritma yang khusus dengan tahapan dan konsiderasi informasi yang digunakan berbeda pula satu sama lain.

Dengan adanya *virtual credit card* yang keamanannya dianggap setingkat di atas kartu kredit umum, maka masalah yang ingin kami bahas adalah penciptaan dan keamanan yang dimiliki oleh kartu-kartu virtual ini. Poin-poin yang akan kami bahas meliputi :

1. Apa yang membedakan VCC dari kartu kredit pada umumnya?
2. Bagaimana algoritma pembuatan angka VCC?
3. Sistem keamanan apa yang dipakai dalam proses transaksinya?

Melalui penelitian ini, kami berharap untuk mengetahui seluk-beluk *virtual credit card*, algoritma yang digunakan untuk menciptakan VCC, dan struktur yang diimplementasikan oleh VCC jika dibandingkan dengan penggunaan kartu kredit biasa.

1.2. Tinjauan Pustaka

1.2.1. Virtual Credit Card

Virtual credit card (VCC) merupakan salah satu penggunaan credit card tanpa bentuk fisik, seperti layaknya internet banking. **(Acharjya, Mitra, & Zaman, 2022)**. VCC hanyalah sebuah kumpulan angka

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

yang dibentuk oleh layanan perbankan untuk para konsumen yang ingin melakukan pembayaran transaksi online tanpa menggunakan kartu fisik, dimana penggunaannya dapat digunakan secara *one-time* atau berkali-kali dikarenakan adanya expiry date pada *virtual credit card* **(P & R, 2015)**.

1.2.2. Cyber Crime

Kejahatan siber merupakan kejahatan yang tersebar luas di internet, menggunakan komputer sebagai alat atau sebagai korban yang ditargetkan **(Dashora, 2011)**. Komputer dapat digunakan dalam hal tindak kejahatan seperti penyerangan terhadap perangkat lain, *scamming*, *trojan*, *phising, cyber fraud*, pencurian data, hingga merusak komponen komputer itu sendiri dengan menggunakan identitas orang lain untuk dituduh.

Meluasnya kejahatan siber perlu ditahan dengan keamanan teknologi. Adanya pencegahan untuk tidak terkena serangan siber dengan melindungi sistem pada komputer dengan menggunakan fitur *firewall, software anti-virus*, dan keperluan yang menunjang keamanan **(Adomi & Igun, 2008)**.

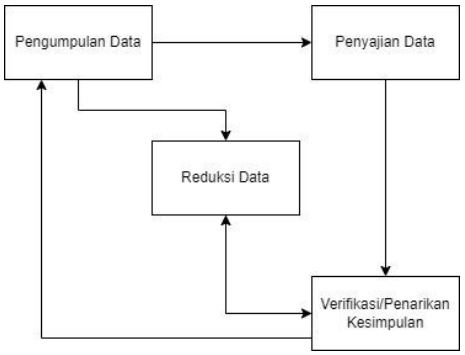
1.2.1. Credit Card Fraud

Credit card fraud atau pencurian atau pengaksesan secara illegal terhadap kartu kredit suatu individu merupakan salah satu tindakan kejatan siber. Kejahatan ini cukup membawa masalah besar, terutama pada penggunaan kartu kredit pada saat melakukan transaksi di e-commerce atau secara online. Kejahatan tersebut dapat dikategorikan menjadi tiga hal; *card related fraud* merupakan penipuan terhadap kehilangan akses dan pemalsuan kartu kredit*, internet related fraud* merupakan website yang menyediakan kartu kredit secara illegal*,* dan *merchant related fraud* merupakan penipuan yang melibatkan pedagang atau *platform* pembelian **(Verma, Singh, Singh, & Laxmi, 2014)**.

1.3. Metodologi

1.3.1. Analisis Data Kualitatif

Analisis data kualitatif meliputi pengumpulan data, reduksi data, penyajian data, dan penyimpulan hasil data dengan lingkup studi yang dipersempit dan analisis tersebut dikembangkan bedasarkan pertanyaan analitik (Rijali, 2018). Pertanyaan yang diajukan berawal dari pertanyaan yang mendasar, hingga pertanyaan akan bersifat detail untuk mengulik informasi terpenting (Raco, 2010).



Gambar 1 Langkah-langkah analisis data kualitatif

Tahap analisis data dimulai dengan pengumpulan data berdasarkan studi dan permasalahan yang telah ditentukan tujuan penelitiannya. Data yang dimaksud dapat berupa gambar, teks, foto, dan angka yang tidak bersifat kuantitatif atau hitungan. Data yang didapatkan akan dianalisis dan dikategorisasikan bedasarkan berdasarkan karakteristik informasi, dilakukannya reduksi data dari informasi yang diperoleh. Sehingga data akan di verifikasi dan disimpulkan dalam bentuk laporan penelitian.

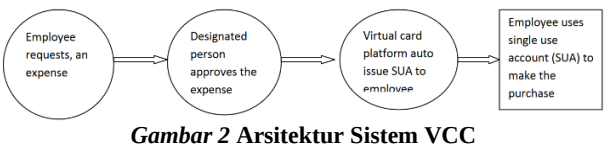
1.3.2. Studi Literatur

Studi literatur atau studi kepustakaan merupakan awal dari proses analisis, dimana pengumpulan data hanya berupa buku dan dokumen yang menyimpan informasi mengenai permasalahan yang ingin diteliti. Studi pustaka merupakan langkah awal untuk menyiapkan kerangka penelitian dengan memanfaatkan sumber perpustakaan untuk mencari informasi yang bersifat data sekunder **(Zed, 2014)**.

Sumber data yang penulis gunakan dalam menggunakan pendekatan studi literatur berasal dari indeks jurnal ilmiah dan buku-buku referensi. Indeks jurnal ilmiah berupa artikel yang menyediakan informasi dan teori yang berkaitan dengan tujuan penelitian. Buku-buku referensi dapat berupa buku mengenai informasi spesifik dengan data yang terfokus pada detail tertentu **(Zed, 2014)**.

2. Pembahasan

Sebelum membandingkan algoritma keamanan virtual credit card, perlu diulas terlebih dahulu *framework* yang diajukan dalam setiap penelitian yang telah dilakukan.

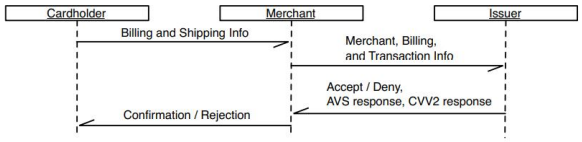


Gambar 2 **Arsitektur Sistem VCC**

Kumar, Kumar, Raj dan Shah (Kumar, Kumar, Raj, & Shah, 2018) berpendapat bahwa VCC yang diciptakan umumnya tidak digunakan dalam jumlah banyak dikarenakan jangka waktu kadaluarsa yang

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

mengekang penggunaan *virtual credit card*. Meskipun begitu, alur dari pemakaian *virtual credit card* tidak jauh beda dari penggunaan kartu debit karena bisa diisi terlebih dahulu sebelum digunakan. Bagi para pemilik kartu yang ingin memiliki *virtual credit card*, mereka mengajukan permintaan pembuatan *virtual credit card* dengan saldo tertentu, kemudian pemilik kuasa mengizinkan ajuan tersebut dan rekening sekali pakai yang akan menjadi *virtual credit card* nantinya pun diciptakan. Pendapat ini mengasumsikan bahwa *virtual credit card* yang telah diciptakan hanya mampu bertahan selama dua puluh empat jam sebelum kadaluarsa serta sangat mengandalkan pemilik *virtual credit card* memiliki *smartphone* karena harus memasukkan kode OTP untuk verifikasi.



Gambar 3 *Alur sistem VCC menuju merchant dan issuer*

Virtual credit card yang diusulkan oleh peneliti Molloy, Li, dan Li (Molloy, Li, & Li, 2007) terbagi menjadi tiga pihak yang terikat dalam proses virtual credit card; *cardholder*, *merchant*, dan *issuer*. *Cardholder* akan melakukan pengiriman informasi *virtual credit card* yang dipakai kepada merchant. Merchant akan mengirim akan mengirim informasi pembelian dan virtual credit card yang didapatkan ke *issuer*. Mereka merumuskan prototipe algoritma penentu nomor *virtual credit card* menggunakan Java 2 MicroEdition yang diuji kemampuannya melalui ponsel-ponsel lama yaitu Sony Ericsson z520a dan Nokia 6102i. Parameter seperti nomor rekening pemilik *virtual credit card*, tanggal kadaluarsa *virtual credit card*, limit transaksi kartu, dan password *virtual credit card* digunakan untuk menentukan kode *virtual credit card* dan CVV_2 yang akan dipakai oleh pengguna. Sistem rumusan ini tidak memikirkan keamanan kartu yang terancam akan disalahgunakan secara ilegal oleh suatu merchant dengan cara pemakaian *virtual credit card* berulang karena mereka berasumsi bahwa penyalahgunaan berulang akan ditangani oleh hukum yang berlaku atas transaksi tersebut.

Penelitian tersebut memastikan bahwa *virtual credit card* hanya dapat digunakan untuk sekali transaksi, sehingga pengguna/cardholder dapat membentuk nomor *virtual credit card* berulang kali apabila ingin melakukan transaksi online, namun tetap ada limitasi pembuatan *virtual credit card* di setiap *cardholder*.

Pada penelitian Gray, Church, dan Ares (Gray, Church, & Ayres, 2015), komponen dalam virtual credit card paling utama adalah angka yang terdiri atas kumpulan angka unik kartu kredit. Pada penelitian mereka, digunakan API berupa Java untuk menghasilkan angka acak.

2343 4566 – generated with java.util.Random
1223 5634 – generated with java.util.Date
2343 4566 1223 5634 – resulting credit card number

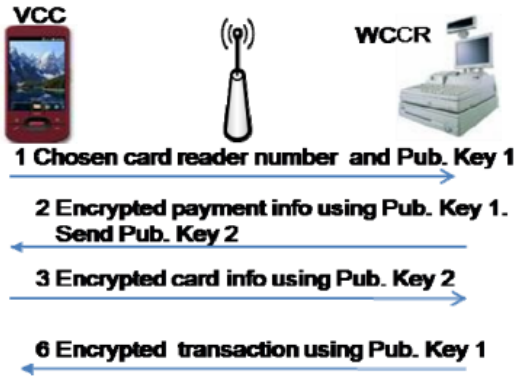
```
//random component
Random random=new Random(16);
long rand = random.nextLong()*random.nextLong();

//unique component - to be contained in a for loop

java.util.Date d = new java.util.Date();
long mili = d.getTime();
Long longmili = new Long(mili + rand);
String num = longmili.toString();
card_numbers[i] = num;
```

Gambar 4 *Hasil angka acak menghasilkan nomor VCC menggunakan java.util.Date Package*

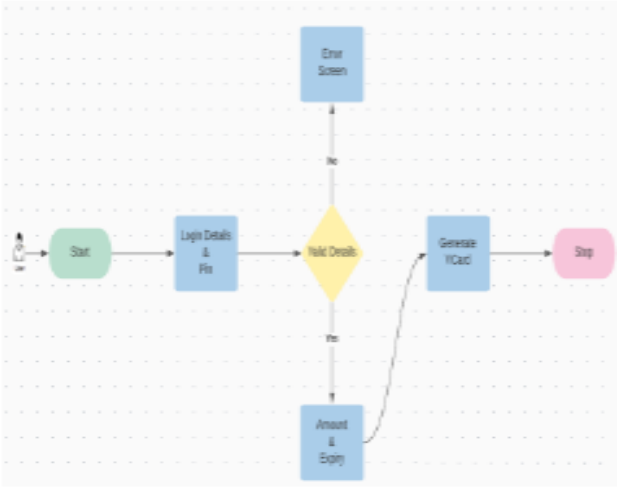
Penelitian tersebut menunjukkan angka virtual credit card terdiri atas 8 angka acak dan 8 angka yang di dapatkan dari methods java getDate() dan getTime(). Hanya saja, pada penelitian ini menunjukkan bahwa methods getDate() akan memungkinkan menghasilkan angka yang identik atau mirip dengan angka lainnya. Sehingga, angka yang di dapatkan tidak akan sepenuhnya 'unik'.



Gambar 5 **Enkripsi VCC menggunakan Public Key ke WCCR**

Kemudian, *framework* yang diusulkan oleh Waraporn (Waraporn, Sithiyavanich, Jiarawattanasawat, & Pakchai, 2009) mengusulkan penggunaan Virtual Credit Card terpusat dalam *mobile phone* saja, sehingga seluruh detail credit card akan tersimpan dalam aplikasi yang terintegrasi. Penggunaan virtual credit card dilindungi dengan keamanan hash code sebagai private key untuk algoritma yang meng-enkripsi informasi credit card sebelum informasi virtual credit card dikirim menuju WCCR. Public key yang dikirim menuju WCCR hanya dapat di-enkripsi oleh *virtual credit card*, sehingga mengurangi adanya kebocoran data dan informasi.

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

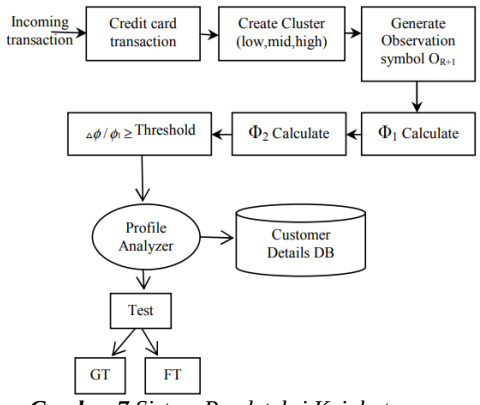


Gambar 6 Diagram Sistem Aplikasi

Pada penelitian Ramya (Ramya, Dr.D.Praveena, Dr.B.Kalpana, & B.Nithish Kumar, 2021), diusulkan arsitektur sistem yang menghubungkan kartu fisik ke dalam kartu virtual yang telah disediakan oleh layanan perbankan visa atau mastercard masing-masing. Penggunaan virtual credit card dapat berupa one-time use/sekali atau menggunakan tanggal kadaluarsa. Jika melewati tanggal kadaluarsa tersebut atau virtual credit card itu telah digunakan dalam transaksi online, virtual credit card akan tidak dapat dipakai lagi.

Apabila terdapata uang yang dimiliki dalam virtual credit card namun telah melewati masa kadaluarsa kartu, secara otomatis uang akan dikirim menuju kartu debit/kredit pemilik virtual credit card.

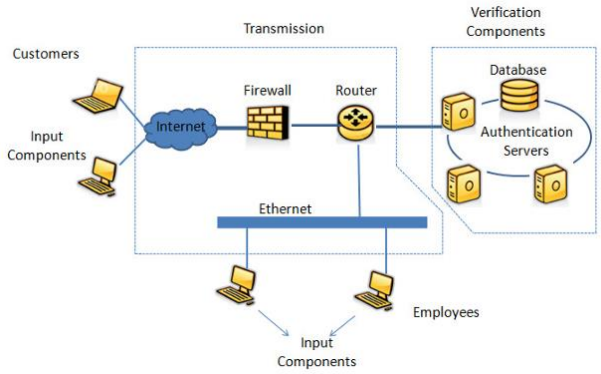
Secara keamanan, P dan R (P & R, 2015) mengusulkan sistem dimana kartu virtual dikeluarkan dan diawasi oleh suatu organisasi. Untuk *virtual credit card* ini, mereka menggunakan sistem keamanan *hidden markov model* dalam aplikasinya dan mengasumsikan bahwa manager organisasi penyedia *virtual credit card* ini akan selalu mendapat notifikasi bahwa kartu sedang dipakai untuk transaksi dan kuasa untuk memperbolehkan maupun menolak transaksi tersebut berada di tangan manager.



***Gambar 7** Sistem Pendeteksi Kejahatan*

Dengan sistem keamanan yang hampir sama juga, Khan, Singh dan Sinhal (Khan, Singh, & Sinhal, 2012) merumuskan pendeteksi kejahatan menggunakan *hidden markov model* dan *K-means*. Sistem pendeteksi ini memprediksikan kejahatan berdasarkan kebiasaan pemilik kartu berbelanja dengan transaksi yang sedang berjalan. Deteksi kebiasaan transaksi ini dibagi menjadi tiga kelompok, yaitu *high spending*, *medium spending* dan *low spending*.

Sistem ini juga dibahas oleh Balamurugan dan Mathiazhagan (Balamurugan & Mathiazhagan, 2015), namun mereka menambahkan algoritma *fuzzy logic* dalam model algoritmanya yang diciptakan dengan bahasa mat lab. *Fuzzy logic* akan mendeteksi kejanggalan atau ketidaksamaan transaksi yang sedang berlangsung dengan riwayat-riwayat transaksi sebelumnya. Penggunaan dari *hidden markov model*, *K-means* dan *fuzzy logic* ini sayangnya terbatas karena hanya mampu mengawasi kejahatan dan membandingkannya dengan data pribadi dan kebiasaan pengguna kartu saja.



***Gambar 8** Skema Keamanan Transaksi Online*

Adapun Naji, Housain, Zaidan, Zaidan dan Hameed (Naji, Housain, Zaidan, & Hameed, 2011) mengusulkan sistem keamanan menggunakan *two-factor authentication* yang terpusat pada penggunaan autentikasi biometrik sidik jari. Sistem ini mengintegrasikan sidik jari yang dimasukkan dengan informasi pemilik kartu dalam basis data saat melakukan transaksi secara online. Usulan ini mengharuskan pemilik kartu untuk memiliki *fingerprint scanner* yang keakuratannya sedang. Data dari *fingerprint* juga dapat diubah oleh pihak selain pengelola database, yaitu oleh pengguna kartu.

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

no	nama jurnal	penulis	parameter yg dipakai	ada arsitektur/alur/grafik?	aplikasi/program yang dipakai	kekurangan
1	Dynamic Virtual Credit Card Numbers	Molloy, Li, Li	untuk generate nomor kartu : limit panjang angka kartu kredit sebenarnya (15/16 digit), informasi nama dan alamat pemilik kartu, password rahasia antara pemegang kartu dan bank, tanggal kadaluarsa VCC, informasi merchant, jumlah transaksi, panjang kode CVV, panjang angka rekening;	Ada	Java 2 MicroEdition (J2ME)	perumusan ini tidak memikirkan merchant yang menyalahgunakan VCC seperti penggunaan berulang kali karena dianggap akan diurus oleh hukum yang berwenang; Asumsi bahwa nama pemegang dan alamat pemegang cukup unik untuk mengidentifikasikan 1 VCC;
2	implement credit card fraudulent detection system using observation probabilistic in hidden markov model	khan, singh, sinhal	untuk deteksi keamanan kartu kredit : menggunakan hidden markov model, rumus saat menggunakan model markov, kebiasaan transaksi pemegang kartu dibandingkan dengan pengeluaran dalam transaksi	Ada	-	Hanya sekedar perumusan matematis tanpa sistem resmi yang mengimplementasikannya, teoritis saja
3	Virtual Credit Card Processing System	Gray, Church, Ares	Menggunakan Java API dengan menggunakan package java.util.Date.package; yaitu method getDate() dan getTime() untuk menghasilkan angka acak pada virtuak credit card number	Ada	Java API	Perumusan ini hanya menentukan angka acak untuk menghasilkan nomor virtual credit card. Akurasi dan angka 'unik' yang dihasilkan tidak terlalu baik untuk diimplementasikan karena dapat memungkinkan menghasilkan hasil angka ganda
4	An Analysis on Making Secure Payment using Virtual Credit Card Technology for Enhancing Data Security	Kumar, Kumar, Raj, Shah	Perbandingan fisik dari kartu kredit dan VCC, alur dari penggunaan VCC	Ada	-	Perumusan hanya analisis alasan-alasan umum mengapa VCC lebih aman, tidak ada penelitian spesifik atau penciptaan sistem khusus buatan sendiri
5	An Unlinkable Anonymous Payment Scheme based on near field communication	Jia Ning Luo, Ming Hour Yang, Szu-Yin Huang	Membentuk skema *anonymous payment* dengan membentuk virtual bank account secara terahasiakan, sehingga dapat menghasilkan ajuan transaksi dan virtual credit card secara anonim.	Ada	G3/UMTS	Hanya berupa perumusan dan skema terhadap anonimitas , tidak ada penelitian yang menunjukkan keberhasilan dalam mengimplementasikan teori tersebut.
6	Virtual Card Creation for Secured Transaction	Manikandan, Latha	sistem penggunaan VCC, penggunaan VCC bisa berulang, penjelasan hidden model markov lebih detail, asumsi VCC dibuat oleh sebuah organisasi untuk klien maka manager organisasi akan mendapat notifikasi mengenai pemakaian VCC dan bisa memilih opsi untuk menerima transaksi atau menolak.	Tidak	-	System ini tidak memakai platform aplikasi khusus untuk generate angka VCC, hanya perlu verifikasi dari organisasi yang mengeluarkan VCC-nya
7	Security Improvment of Credit Card Online Purchasing System	Naji, Housain, Zaidan,Zaidan, Hameed	penggunaan informasi kartu kredit dan autentikasi biometrik dalam autentikasi 2 faktor, integrasi sistem pembelian online dengan biometrik fingerprint, harga dari fingerprint menengah ke bawah harganya dengan	Ada	program fingerprint, database, webpage, apache server	keakuratan fingerprint based authentication tidak tinggi, informasi dalam database bisa dibobol karena harus open dan mampu dimanage oleh pemilik kartu, pemilik kartu harus memiliki alat fingerprint

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

			akurasi menengah dan kompatibel dengan banyak komputer			
8	Credit Card Security System and Fraud Detection Algorithm	Al-Smadi	pendataan informasi pemegang kartu kredit, shared password antaran penyedia kartu dan pemilik, informasi transaksi (kordinat pengguna kartu, waktu transaksi, nomor IP/IMEI)	Ada	web server, database, koneksi internet	memiliki limit waktu untuk melakukan transaksi kalau tidak informas kartu akan hangus dan harus membuat ulang,
9	Contactless Credit Cards Payment Fraud Protection by Ambient Authentication	Yang, Luo, Vijayalakshmi, Shalinie	Adaptasi perintah EMV yang sudah ada dan memakai reserved-for-future-use (RFU) field dalam parameter perintah utk kirim pesan; verifikasi dengan metode ambient authentication. hp dengan NFC bisa menggunakannya, token pengirim kode, bank pemegang rekening, bank pengelola kartu, merchant	Ada	POS terminal, smartphone dengan nfc, aplikasi pembayaran	Pembayaran harus memiliki NFC, fokus dengan mobile payment saja
10	Credit Card Transaction Fraud Detection System Using Fuzzy Logic and K-Means Algorithm	Balamurugan, Mathiazhagan	K-means mengelompokkan data berdasar kemiripan nilai transaksi mereka (pengelompokan ada 3: tinggi, sedang, redah), data yang dibutuhkan adalah no transaksi, tanggal, waktu, jumlah barang, limit transaksi, umur, alamat shipping, alamat pelanggan.	Tidak	Mat lab language	Mendeteksi hanya tergantung kebiasaan, tidak bisa antisipasi jika pelanggan suatu saat ingin melakukan transaksi yang berbeda dari kebiasaan lama mereka
11	Virtual Credit Cards on Mobile for M-Commerce Payment	Waraporn, Sithiyanavich, Jiarawattanasawat, Pakchai	Menggunakan metode enkripsi public key dan private key pada saat transaksi menggunakan virtual credit card menuju WCCR merchant, sehingga data akan terenkripsi oleh public key, dan public key yang tersedia tidak hanya satu	Ada	Android SDK dan Dalvik Virtual Machine	Sistem yang diajukan hanya menggunakan sistem bluetooth, sehingga tidak layak untuk diimplementasikan kedepannya karena lemahnya jaringan bluetooth

Tabel 1 Comparative Analysis

3. Kesimpulan

Penggunaan sistem dan algoritma memiliki fungsi dan kelebihannya masing-masing, sehingga perlu dilakukan perbandingan dengan studi literatur untuk melakukan analisis. Analisis penelitian ini ditujukan untuk membandingkan algoritma dan arsitektur dari virtual credit card untuk menyimpulkan keamanan dari masing-masing teori, terutama pada transaksi antara pengguna virtual credit card dengan merchant. Hasil yang diperoleh berupa alur pemakaian *virtual credit card* dalam transaksi dimana umumnya transaksi melibatkan tiga pihak untuk berjalan lancar, yaitu pihak pengguna kartu yang melakukan transaksi dengan merchant, kemudian merchant akan mengirimkan permohonan tagihan belanja dan *provider* kartu sebagai pemantau transaksi dan penentu apakah transaksi tersebut dapat disetujui atau tidak ditinjau dari informasi yang ada. Lalu, terdapat berbagai macam cara untuk menentukan nomor *virtual credit card* dengan penggunaan rata-ratanya sekali transaksi saja dan hanya bisa bertahan dalam jangka waktu yang lebih singkat dari kartu kredit biasa. Hasil terakhir yang kami dapat adalah sistem keamanan apa saja yang diusulkan untuk melindungi transaksi tersebut, dengan teknik *hidden markov model* dan K-means sebagai opsi yang cukup sering digunakan sebagai metode pendeteksi kejahatan di antara literatur yang telah kami telaah.

Daftar Pustaka

Acharjya, D. P., Mitra, A., & Zaman, N. (2022). *Deep Learning in Data Analytics.* Springer Nature Switzerland.

Adomi, & Igun. (2008). Combating Cyber Crime in Nigeria. *Electronic Library*, 716-725.

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

Dashora, K. (2011). Cyber Crime in the Society: Problems and . *Journal of Alternative Perspectives in the Social Sciences*, 240-259.

Douglas, J. (2018). *Manufacturing Debt : A History of the Bank Credit Card Infrastructure*. Toronto: Department of History University of Toronto.

Hendarsyah, D. (2020). Analisis Perilaku Konsumen dan Keamanan Kartu Kredit Perbankan. *Jurnal Perbankan Syariah*, 12.

Hermogeno, D. L. (2019). E-Commerce : History and Impact on the Business and Consumers. *IJESC*, 5.

Kumar, A., Kumar, R., Raj, N., & Shah, A. (2018). An Analysis on Making Secure Payment using Virtual Credit Card Technology for Enhancing Data Security. *International Journal of Computer Applications*, 3.

Molloy, I., Li, J., & Li, N. (2007). Dynamic Virtual Credit Card Numbers. *Lecture Notes in Computer Science*, 208-223.

P, M., & R, L. (2015). Virtual Card Creation for Secure Transaction. *International Journal of Trend in Research and Development*.

Permana, A. E., Reyhan, A. M., Raffli, H., & Rakhmawati, N. A. (2021). Analisa Transaksi Belanja Online pada Masa COVID-19. *Jurnal TEKNOINFO*, 6.

Raco, J. (2010). *Metode Penelitian Kualitatif : Jenis, Karakteristik, dan Keunggulannya.* Jakarta: PT Gramedia Widiasarana Indonesia.

Rijali, A. (2018). Analisis Data Kualitatif. *Jurnal Alhadharah*, 81-95.

Verma, S., Singh, A., Singh, D. D., & Laxmi, V. (2014). Computer Forensics in IT Audit and Credit Card . *International Conference on Computing for Sustainable Global Development (INDIAcom)*, 730-733.

Waraporn, N., Sithiyavanich, M., Jiarawattanasawat, H., & Pakchai, N. (2009). Virtual Credit Cards on Mobile for M-Commerce Paymen. *IEEE International Conference on e-Business Engineering*, 241-246.

Zed, M. (2014). *Metode Penelitian Kepustakaan.* Jakarta: Yayasan Pustaka Obor Indonesia.