Jurnal Politeknik Caltex Riau
http://jurnal.pcr.ac.id

Aplikasi Notifikasi Mobile Untuk Pencegahan Fraud

Azhari[1], Chandra Saha Dewa Prasetya[2] dan Achmad Jeihan Pahlevi[3]

[1] Departemen Ilmu Komputer dan Elektronika FMIPA UGM, email: arisn@ugm.ac.id
[2]Program Studi Ilmu Komputer FMIPA UGM, email: chandra.saha.d@mail.ugm.ac.id
[3]Program Studi Ilmu Komputer FMIPA UGM, email: achmad.jeihan.p@ mail.ugm.ac.id

Abstrak

Telepon mobile pintar sudah banyak dimanfaatkan dalam melakukan transaksi perbankan misalnya melihat saldo rekening dan riwayat transaksi, transfer dana antar rekening, atau membayar tagihan secara online. Dalam beberapa tahun belakangan, peretasan transaksi dari perbankan melalui kartu kredit meningkat sangat tinggi, misalnya pada tahun 2013, sekelompok hacker berhasil membobol Bank Muscat yang berada di negara Oman dan menyebabkan kerugian senilai 45 juta USD. Dalam paper ini dikembangkan sebuah prototipe notifikasi pencegahan kejahatan fraud berbasis mobile. Sampel data digenerate dari sampel random transaksi nasabah dan beberapa data nasabah. Prototype kemudian diuji pada berbagai kondisi normal, dan ekstrim. Berdasarkan hasil pengujian, didapat beberapa variasi notifikasi fraud, seperti pada jam sibuk dan tidak sibuk. Notifikasi yang dikirimkan pada jam sibuk relatif lebih cepat dibandingkan saat jam tidak sibuk.

Kata kunci: *Mobile, Transaksi, Fraud,*

Abstract

Smart mobile phones are already widely used in banking transactions eg, view account balances and transaction history, transfer funds between accounts or paying bills online. In recent years, the hacking of banking transactions through credit cards rose to very high, for example in 2013, a group of hackers managed to break into Bank Muscat which are in Oman and caused damage worth 45 million USD.In this paper developed a prototype notification of fraud based mobile crime prevention. Sample data is generated from a random sample of customer transactions and some customer data. Prototype then tested on various normal conditions, and extreme.Based on test results, obtained some variation of the notification of fraud, such as during rush hour and not busy. Notifications submitted at busy times faster relative to the current off-peak hours.

Keywords: *Mobile, Transaction, Fraud*

1. Pendahuluan

Telepon mobile pintar saat ini digunakan untuk membantu berbagai sektor kehidupan manusia salah satunya adalah sektor perbankan. Dengan memanfaatkan telepon mobile pintar, proses e-banking dapat meningkatkan efisiensi, menurunkan biaya, dan layanan 24 jam [1]. Nasabah dapat melakukan transaksi dari mana saja selama terhubung dengan internet. Tidak seperti cabang bank yang buka hanya saat jam kerja, e-banking juga memungkinkan nasabah untuk melakukan transaksi keuangan kapan saja.

Dokumen diterima pada 16 Oktober, 2016
Dipublikasikan pada 16 Mei, 2017

Hampir setiap bank saat ini menerapkan layanan e-banking yang didukung dengan teknologi aplikasi mobile untuk menarik nasabah menggunakan layanan tersebut. Disisi lain, nasabah dapat memilih bank mana yang dapat membantu nasabah dalam bertransaksi. Kemananan, kecepatan transaksi, tampilan yang mudah digunakan merupakan beberapa faktor yang mempengaruhi nasabah untuk memilih bank tertentu [2].

Namun dalam beberapa tahun belakangan, jumlah kejahatan siber yang menyerang sektor perbankan semakin tinggi. Sebagai contoh pada tahun 2008, Inggris mengalami kerugian sebanyak 53 juta dolar karena serangan hacker pada online bank. Menurut data dari Reserve bank of India (RBI) jumlah kerugian karena serangan hacker telah meningkat dua kali lipat dalam empat tahun terakhir [3].

Untuk mencegah terjadinya kejahatan fraud, sebuah prototipe notifikasi berbasis mobile dikembangkan untuk medeteksi apabila sebuah transaksi dicurigai sebagai fraud. Sebuah notifikasi akan dikirimkan pada mobile pengguna untuk memberikan konfirmasi apakah transaksi tersebut merupakan fraud atau bukan.

2. Penelitian Sebelumnya

Melakukan penelitan tentang metode pendeteksi fraud dan intrusi untuk e-commerce pada mobile[4]. Sebuah model generik dikembangkan bernama “Activity Event-Symptoms” (AES) untuk mendeteksi fraud dan serangan intrusi yang terjadi saat proses pembayaran pada e-commerce menggunakan telepon mobile. AES diuji menggunakan berbagai studi kasus, yaitu menggunakan jaringan wireless dan jaringan GSM/CDMA. Setelah melakukan penelitian, peneliti mendapat kesimpulan bahwa menggunakan teknik ini, proses identifikasi fraud berjalan lebih cepat dibandingkan dengan teknik lain.

Selanjutnya, [5] melakukan penelitian tentang pendeteksi fraud pada mobile payment menggunakan analisis kebiasaan pengguna. Peneliti menganalisis penyimpangan dari perilaku pengguna untuk mengenali anomali yang mengindikasikan terjadinya penyalahgunaan layanan terkait money laundry. Penelitian ini menggunakan metode predictive security analyzer dan algoritma jaringan saraf tiruan untuk mengidentifikasi pola perilaku yang menyimpang. Hasil penelitian ini menunjukkan bahwa predictive security analyzer cukup efektif saat simulasi, namun jika diaplikasikan pada sistem sebenarnya, perlu adanya perbaikan untuk menghindari noise yang mungkin terjadi.

Di tahun berikutnya, [6] melakukan penelitian mengenai pendeteksi fraud pada transfer rekening pada telepon mobile. Peneliti menggunakan metode yang sama dengan penelitian sebelumnya yaitu predictive security analyzer, namun algoritma yang digunakan adalah algoritma FCD. Hasil dari penelitian ini menunjukkan nilai yang cukup tinggi yaitu nilai presisi 99.81% dan recall 90.81%.

Yang terbaru, [7] mengembangkan arsitektur sebuah sistem keamanan “Host Card Emulation” (HCE) yang memanfaatkan NFC pada pembayaran menggunakan telepon mobile. Dengan menggunakan HCE, maka data perbankan yang dikirimkan melalui NFC seperti nomor kartu kredit, tanggal valid, kunci kriptografi dapat dilindungi.

3. Online Banking

Online banking adalah sebuah rangkaian proses dimana nasabah bank login ke website dari suatu bank melalui browser yang terinstall pada komputer atau mobile nasabah dan melakukan berbagai transaksi keuangan.

Pada tahap dasar, internet banking dapat diartikan mengatur sebuah website dari bank untuk memberikan informasi mengenai layanan dan produknya. Pada tahap lanjut, internet

banking melibatkan berbagai fasilitas yang diberikan seperti mengakses akun, melakukan transfer uang ke rekening lain, membeli produk secara online, atau membayar berbagai tagihan elektronik. Hal ini merupakan online banking yang bersifat transaksional.

Untuk berbagai transaksi online, user akan menggunakan komputer atau smartphone dan membuka browser kemudian memasukkan id atau Personal Identification Number (PIN) dan Password untuk masuk ke rekening user. SSL (Secure Socket Layer) kemudian akan mengenkripsi data yang dikirimkan dari komputer/smartphone user ke server bank. Sever bank akan mendekripsi berbagai data yang diterima seperti autentikasi akun, transfer akun, dan sebagainya.

4. Cybercrime Pada Transaksi Bank Menggunakan Mobile Phone

Mobile banking dan internet banking mempunyai banyak kelebihan seperti menghemat waktu, menurunkan biaya, dapat digunakan kapan saja, dan mudah digunakan [8]. Namun, salah satu tantangan di bidang mobile banking adalah masalah keamanan. Akhir-akhir ini, jumlah kejahatan cybercrime yang menyerang bank semakin meningkat.

Cybercrime melibatkan kegiatan kriminal seperti pemalsuan, penipuan, pencurian, kerusakan dan pencemaran nama baik serta web defacement, hacking, web jacking & web stalking yang telah berevolusi dalam akibat dari penyalahgunaan komputer. R Nagpal dari sekolah Asia cyber law mendefinisikan cybercrime sebagai "tindakan melanggar hukum di mana komputer sebagai alat atau sasaran atau keduanya" dimana komputer yang digunakan tidak hanya dimaksudkan untuk komputer desktop, tetapi juga termasuk smartwatch, smartphone, Personal Digital Assistant (PDA) dan sejumlah gadget lain. Serangan cybercrime dapat mengakibatkan bahaya yang mengerikan seperti lalu lintas kontrol udara, pasar saham, sistem perbankan [9].

Berikut adalah beberapa serangan cybercrime yang mungkin terjadi pada mobile banking :

4.1 Distributed Denial of service (DDOS)

DDOS adalah salah satu serangan yang sering dilakukan pada sistem bank. Sebelum melakukan serangan, hacker akan menyerang jaringan bank dengan melakukan scan pada port yang terbuka [10].

4.2 Malware

Malware adalah istilah untuk software yang dibuat untuk tujuan kejahatan. Malware dapat melakukan operasi berbahaya seperti mencuri informasi akun target [11].

4.3 TCP/IP Spoofing

Dengan memalsukan alamat ip target, pelaku kejahatan mendapatkan akses yang tidak sah terhadap sebuah telepon mobile atau jaringan [12].

4.4 Backdoor

Backdoor adalah sebuah celah yang diciptakan untuk menghindari mekanisme keamanan. Backdoor biasanya dibuat programmer untuk menyelesaikan permasalahan pada program. Sayangnya, backdoor sering dimanfaatkan pelaku kejahatan untuk mendapatkan akses dengan menerobos sistem keamanan [13].

4.5 Tampering

Tampering adalah sebuah modifikasi pada produk sehingga produk tersebut menjadi berbahaya terhadap konsumen [14].

4.6 Exploits

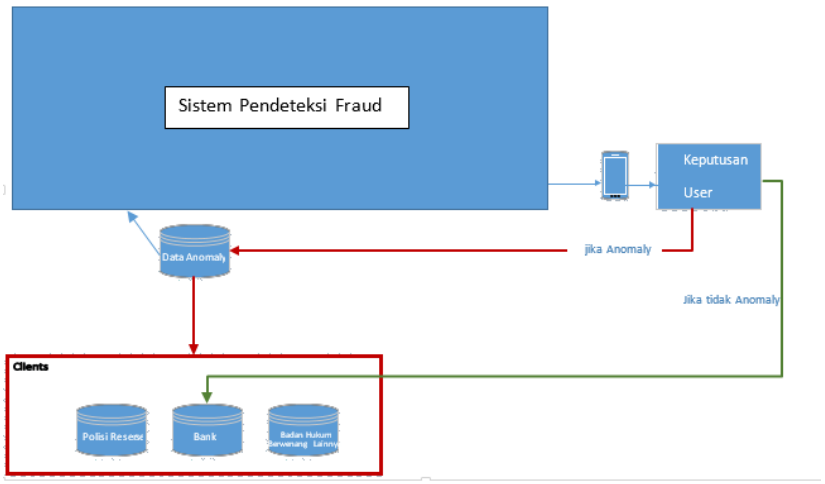
Exploits adalah sebuah bagian software atau data yang menjadi celah yang dapat digunakan pelaku kejahatan untuk menyusup kedalam sistem atau jaringan [15].

4.7 Trojan

Trojan merupakan sebuah program tanpa izin yang dapat menghapus, memblokir, mengubah, dan mengopi data. Namun trojan tidak dapat mereplikasi dirinya sendiri seperti virus atau worm [16].

5. Usulan model notifikasi pencegahan fraud

Berikut adalah usulan model sistem notifikasi yang kami rancang. Seperti yang ditunjukkan pada Gambar 1, model sistem yang dirancang akan terdiri dari beberapa komponen yaitu sistem pendeteksi fraud dan aplikasi notifikasi mobile. Sistem pendeteksi fraud akan dirancang untuk melakukan prediksi outlier dari data source. Sistem pendeteksi fraud dibuat menggunakan algoritma autoencoding. Model akan ditrain dan menghasilkan prediksi transaksi yang bersifat outlier yang dicurigai sebagai transaksi fraud.



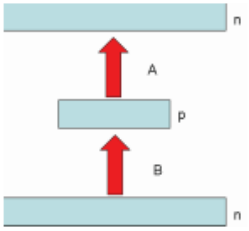
Gambar 1. Usulan Model Sistem Notifikasi

Aplikasi akan berguna untuk mengirimkan transaksi yang diprediksi oleh fraud detector yang dicurigai sebagai fraud ke smartphone user. Aplikasi akan membantu user untuk membuat keputusan apakah transaksi tersebut merupakan fraud atau bukan. Apabila transkasi tersebut merupakan fraud maka transaksi tersebut dapat dilaporkan ke polisi, bank, atau badan hukum berwenang lainnya. Sehingga , apabila user mendapatkan notifikasi dan transaksi tersebut tidak dilakukan oleh user/nasabah tersebut, maka user dapat membatalkan transaksi yang terjadi.

6. Sistem Pendeteksi Fraud

Pada paper ini kami mengusulkankan autoencoder untuk mendeteksi outlier yang dianggap sebagai fraud pada transaksi perbankan. Autoencoder adalah sebuah sirkuit pembelajaran sederhana untuk mengubah input menjadi output dengan jumlah penyimpangan yang minimum [17]. Tujuan dari autoencoder adalah mempelajari representasi dari sekumpulan data. Untuk menjelaskan framework secara umum, sebuah autoencoder *n/p/n* didefinisikan dengan sebuah tuple *n*, *p*, *m*, F, G, *A*, *B*, *X*, Δ dimana :

1. F dan G adalah sebuah himpunan.
2. *n* dan *p* adalah bilangan bulat positif dimana $0 < p < n$.
3. *A* adalah fungsi class dari G^p ke F^n.
4. *B* adalah fungsi class dari F^n ke G^p.
5. $X = \{x_1, \ldots, x_m\}$ adalah sebuah himpunan dari vektor m (training) dalam F^n. Ketika terdapat target eksternal, $Y = \{y_1, \ldots, y_m\}$ menyatakan himpunan target vektor yang sesuai pada F^n.
6. Δ adalah sebuah fungsi penyimpangan (contohnya: L_p norm, Hamming distance) yang didefinisikan pada F^n.



Gambar 2. Arsitektur autoencoder *n/p/n*

Untuk setiap A ∈ *A* dan B ∈ *B*, autoencoder melakukan transformasi sebuah input vektor $x \in F^n$ ke sebuah output vektor $A \circ B(x) \in F^n$ (Gambar 2). Permasalahan autoencoder adalah untuk menemukan A ∈ *A* dan B ∈ *B* yang meminimalkan fungsi distorsi secara keseluruhan :

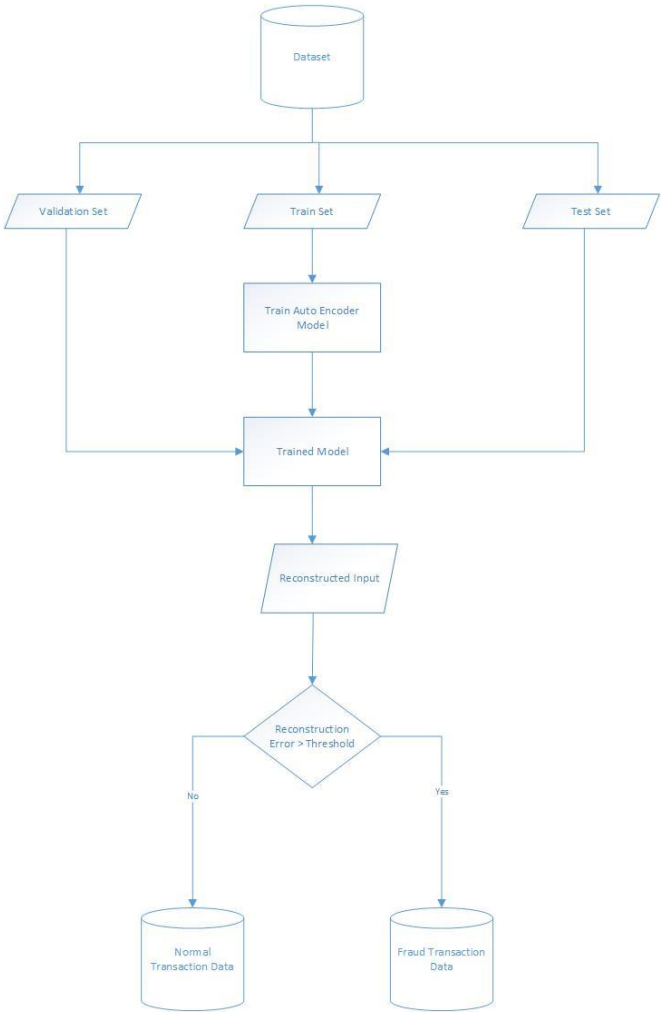
$$\min E(A,B) = \min_{A,B} \sum_{t=1}^{m} E(x_t) = \min_{A,B} \sum_{t=1}^{m} \Delta(A \circ B(x_t), x_t) \quad (1)$$

Pada kasus auto-associative, ketika terdapat target eksternal y_t, maka fungsi minimalisasi adalah

$$\min E(A,B) = \min_{A,B} \sum_{t=1}^{m} E(x_t, y_t) = \min_{A,B} \sum_{t=1}^{m} \Delta\left(A \circ B(x_t), y_t\right) \quad (2)$$

dengan catatan $p < n$ saat autoencoder mencoba mengimpementasikan beberapa jenis kompresi atau ekstraksi fitur.

Pada penelitian ini, metode semi supervised learning digunakan dengan mentrain auto encoder menggunakan data transaksi yang dilabeli/dianggap sebagai transaksi “normal” , yaitu transaksi. Autoencoder akan merekonstruksi ulang input dengan dimensi m menjadi output dengan dimensi yang sama. Normalnya , transaksi yang “normal” akan menghasilkan nilai error yang relatif kecil atau < threshold yang ditentukan. Arsitektur sederhana dari metode yang kami usulkan ditunjukkan pada Gambar 3.



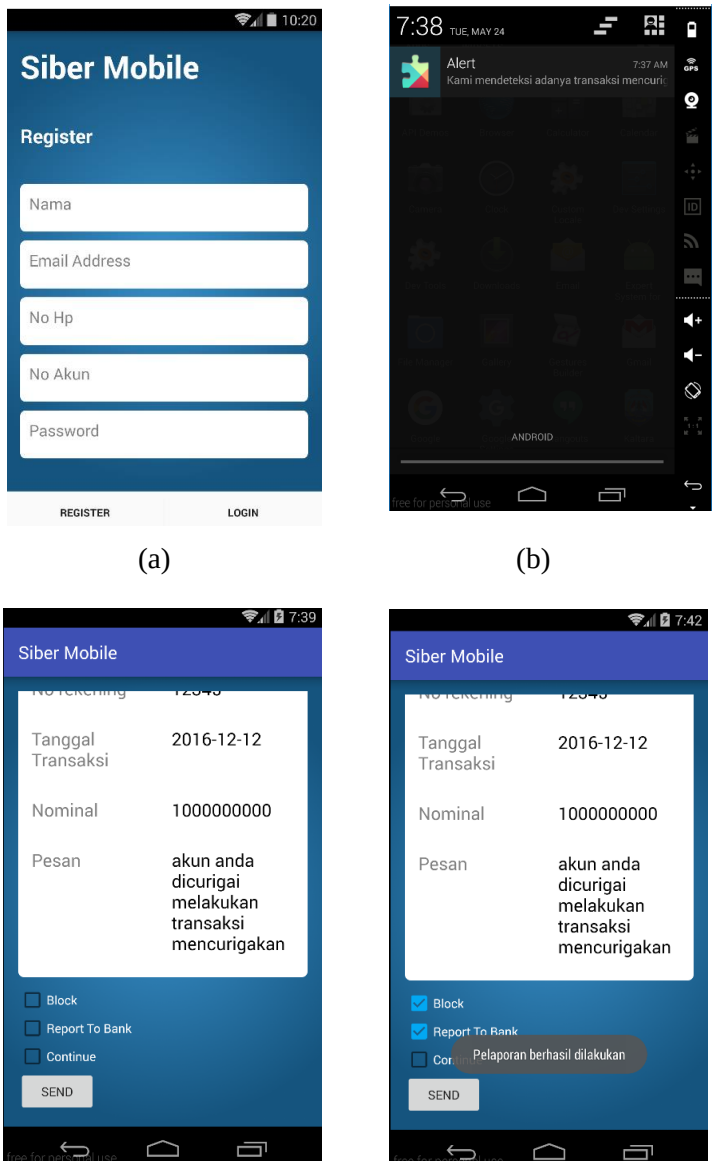
Gambar 3. Usulan Sistem Pendeteksi Fraud

Feed forward neural network dan backpropagation algorithm digunakan dalam proses pelatihan. Fungsi loss dihitung menggunakan fungsi logistik dengan mengambil rata-rata dari semua cross-entropies pada sample. Misalnya kita memiliki N samples, karena kita ingin menyelesaikan masalah binary classification, untuk setiap sample diberi label{-1,+1} ini sering disebut sebagai binary cross entropy [17] . Fungsi loss didefiniskan sebagai berikut:

$$L(\mathbf{w}) = \frac{1}{N}\sum_{n=1}^{N} H(p_n, q_n) = -\frac{1}{N}\sum_{n=1}^{N}\left[y_n \log \hat{y}_n + (1-y_n)\log(1-\hat{y}_n)\right], \quad (3)$$

dimana , $\hat{y}_n \equiv g(\mathbf{w}\cdot\mathbf{x}_n)$ dengan g (z) fungsi logistic.

7. Hasil dan Pembahasan



Gambar 4. Hasil Aplikasi Notifikasi

Seperti yang ditunjukkan pada Gambar 4(a), saat pertama kali menggunakan aplikasi, user akan diminta untuk melakukan registrasi yang berisi data nama, nomor rekening, password, dan alamat user. Data user akan dikirimkan melalui Application Programming Interface ke server google untuk mendapatkan registrationID, kemudian data user dan registrationID akan disimpan ke server. RegistrationID akan digunakan untuk mengirimkan notifikasi ke dalam smartphone user.

Setelah user berhasil login, maka aplikasi akan berjalan secara background service. Pada Gambar 4(b) menunjukkan ada transaksi yang terdeteksi sebagai fraud, kemudian notifikasi dikirimkan ke smartphone pengguna.

Saat notifikasi dibuka, maka akan ditampilkan informasi mengenai transaksi yang mencurigakan yaitu nomor rekening, tanggal transaksi, nominal, dan pesan yang dikirimkan seperti pada Gambar 4(c). User dapat melakukan beberapa aksi yaitu melakukan block, melaporkan ke bank, melaporkan ke polisi, atau continue.

Apabila user melaporkan kepada bank atau polisi, maka data transaksi tersebut akan dikirimkan ke bank atau polisi. Pada Gambar 4(d) menunjukkan apabila transaksi tersebut bukan merupakan keinginan pemilik rekening, kemudia dengan mencentang block dan report to bank dan melakukan tap pada tombol send, maka transaksi tersebut akan diblock dan dilaporkan ke bank.

Apabila user benar-benar melakukan transaksi tersebut, maka user dapat melanjutkan transaksi dengan mencentang continue. Transaksi tersebut kemudian dimasukkan ke daftar transksi anomali yang kemudian akan dijadikan model oleh sistem pendeteksi fraud untuk melakukan prediksi lebih baik lagi dengan semakin banyaknya data yang tersedia.

8. Kesimpulan

Online banking menggunakan telepon mobile pintar memberikan kemudahan bagi nasabah untuk melakukan berbagai transaksi keuangan dari mana saja dan kapan saja. Namun ada hal yang perlu diperhatikan saat menggunakan online banking yaitu masalah keamanan. Sebuah prototipe notifikasi berbasis mobile dikembangkan untuk mencegah terjadinya fraud. Saat sistem pendeteksi fraud menprediksi terjadi sebuah transaksi fraud, notifikasi akan dikirimkan ke telepon mobile pintar nasabah secara real time. Kemudian, nasabah dapat melakukan blok dan melaporkan transaksi fraud kepada bank sehingga fraud dapat dicegah.

Daftar Pustaka

[1] M. T. Taghavifard dan M. Torabi. “Factors Affecting the Use of Mobile Banking Services by Customers and Rank them Case Study: Tejarat Bank Branches In Tehran,” *Journal of Business Management Researches,* 2010.

[2] H. Amadeh dan M. Jafarpour. “Study of the Barriers and Strategies for the Development of Electronic Banking in the Country's Private Banks,” *Executive Management Review* 2009.

[3] R.K. Jassal dan R.K. Sehgal. “Online Banking Security Flaws: A Study,” *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3(8). 2013.

[4] P. Venkataram *et al.* “A Method of Fraud & Intrusion Detection for E-payment Systems in Mobile e-Commerce,” *IEEE International Performance, Computing, and Communications Conference,* pp. 395-401, Apr. 2007.

[5] R. Rieke *et al.* “Fraud Detection in Mobile Payments Utilizing Process Behavior Analysis,” *Eighth International Conference on Availability, Reliability and Security (ARES),* 2013, pp. 662-669.

[6] M. Zhdanova *et al.* “No smurfs: Revealing Fraud Chains in Mobile Money Transfers,” *Ninth International Conference on Availability, Reliability and Security (ARES), 2014,* pp. 11-20.

[7] M. Pasquet dan S. Gerbaix. “Fraud on Host Card Emulation Architecture: Is It Possible to Fraud a Payment Transaction Realized by a Mobile Phone Using an "Host Card

Emulation" System of Security?" *Second International Conference on Mobile and Secure Services (MobiSecServ)*, 2016, pp. 1-3.

[8] L. Nosrati dan A.M. Bidgoli. "Security Assessment of Mobile-banking," *International Conference and Workshop on* In *Computing and Communication (IEMCON)*, 2015, pp. 1-5.

[9] D.J. Neufeld. "Understanding Cybercrime," *43rd Hawaii International Conference on System Sciences (HICSS)*, 2010, pp. 1-10.

[10] M.S. Islam. "Systematic Literature Review: Security Challenges of Mobile Banking and Payments System," *International Journal of u-and e-Service, Science and Technology*, vol. *7*(6), pp.107-116, 2010.

[11] Elkhodr *et al.* "A Proposal to Improve the Security of Mobile Banking Applications," *10th International Conference on ICT and Knowledge Engineering (ICT & Knowledge Engineering)*, 2012, pp. 260-265.

[12] W. He. "A Review of Social Media Security Risks and Mitigation Techniques," *Journal of Systems and Information Technology*, vol. *14*(2), pp.171-180, 2012.

[13] W. He. "A Survey of Security Risks of Mobile Social Media Through Blog Mining and an Extensive Literature Search," *Information Management & Computer Security*, vol. *21*(5), pp.381-400, 2013.

[14] P. Judge dan M. Ammar. "Security issues and solutions in multicast content distribution: A survey," *IEEE network*, vol. 17(1), pp.30-36, 2003.

[15] H.U. Khan. "E-banking: Online Transactions and Security Measures," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 7(19), pp.4056-4063, 2014.

[16] R.K. Jassal dan R.K. Sehgal. "Study of Online Banking Security Mechanism in India: Take ICICI Bank as an Example,"

[17] P. Baldi. "Autoencoders, Unsupervised Learning, and Deep Architectures," *ICML unsupervised and transfer learning*, vol. 27(37-50), p.1, 2012

[18] K.P. Murphy. *Machine learning: a probabilistic perspective*. MIT press, 2012.