Model Kepercayaan dengan Menggunakan Perhitungan *Similarity*

Anisa Mardhatillah[1], Diny Wahyuni[2], Detty Purnamasari[3]

[1]Magister Manajemen Sistem Informasi, Universitas Gunadarma
[2]Sistem Informasi, Universitas Gunadarma
[3]Teknologi Informasi, Universitas Gunadarma
Jl. Margonda Raya No.100, Depok
E-mail : mardhatillah.anisa@gmail.com, dwahyuni@staff.gunadarma.ac.id,detty@staff.gunadarma.ac.id

Abstrak

Model kepercayaan berkaitan dengan kepercayaan yang diterapkan dalam kehidupan. Kepercayaan yang bersifat subjektif dan bergantung pada konteks. Kepercayaan secara umum merupakan ukuran keyakinan bahwa suatu entitas akan berprilaku dengan cara yang diharapkan, meskipun kurangnya kemampuan untuk memantau atau mengontrol lingkungan di mana entitas beroperasi. Model kepercayaan dapat diterapkan dalam berbagai metode dan sektor kehidupan. Termasuk dalam penggunaan jejaring sosial. Salah satu metode yang digunakan dalam model kepercayaan adalah *similarity*. *Similarity* memiliki arti kesamaan, kemiripan, persamaan, dan/atau keserupaan. *Similarity* dalam kata adalah mencari kesamaan antara kata masukkan (*input*) dengan kata sumber. Hubungan virtual dibangun di atas metrik yang digunakan untuk menghubungkan pengguna berdasarkan pengalaman mereka dan disebut dengan kesamaan. Berbagai metrik kesamaan telah diterapkan dalam skenario yang berbeda, misalnya, metrik kesamaan pengguna untuk rekomendasi teman di jejaring sosial dan metrik kesamaan topologi untuk prediksi tautan dan deteksi komunitas. Tujuan dari penelitian ini dilakukan adalah untuk mengetahui keterkaitan antara penggunaan model kepercayaan dalam interaksi yang dilakukan, khususnya dalam penggunaan metode *simalirity*. Hasil yang didapat menunjukan bahwa, model kepercayaan dapat menggunakan metode *similarity* untuk implementasi yang lebih luas. Karena jika seseorang memiliki kesamaan terhadap suatu hal, maka orang tersebut cenderung untuk percaya.

Kata Kunci: Model Kepercayaan, *Similarity*, Jejaring Sosial

Pendahuluan

Model kepercayaan erat kaitannya dengan kepercayaan yang diterapkan dalam kehidupan sehari-hari. Kepercayaan bersifat subjektif yang bergantung pada konteks dan bersifat dinamis.

Model kepercayaan merupakan suatu mekanisme khusus yang diperlukan untuk menanggapi profil ancaman tertentu. Profil ancaman adalah sekumpulan ancaman atau kerentanan yang diidentifikasi melalui analisis aliran data berdasarkan kasus penggunaan yang khusus untuk organisasi. Pada dasarnya, profil ancaman mengidentifikasi kemungkinan penyerang dan apa yang mereka inginkan [1].

Model kepercayaan mencakup validasi implisit dan eksplisit dari identitas entitas atau karakteristik yang diperlukan agar peristiwa atau transaksi tertentu terjadi. Bawa dan Singh [2] mengatakan, kepercayaan secara umum adalah ukuran keyakinan bahwa suatu entitas akan berprilaku dengan cara yang diharapkan, meskipun kurangnya kemampuan untuk memantau atau mengontrol lingkungan di mana entitas beroperasi.

Chervany dan McKnight [3], mengategorikan tiga prinsip kepercayaan, yaitu kepercayaan pribadi atau interpersonal, yang menggambarkan kepercayaan antara orang atau kelompok. Ini terkait pengalaman yang dimiliki orang satu sama lain. Kemudian kepercayaan impersonal atau struktural, tidak terikat pada seseorang tetapi timbul dari situasi sosial atau organisasi. Terakhir yaitu kepercayaan disposisional, merupakan suatu sikap umum seseorang terhadap dunia.

Model kepercayaan pertama kali diusulkan oleh Marsh [4] pada tahun 1994 yang mengintegrasikan konsep kepercayaan yang berbeda. Marsh berkonsentrasi pada pemodelan kepercayaan antara dua agen, dengan memperkenalkan pengetahuan, kegunaan, kepentingan, risiko, dan kompetensi yang dirasakan sebagai aspek penting yang terkait dengan kepercayaan. Namun model kepercayaa yang

DOI : http://dx.doi.org/10.32409/jikstik.20.3.2771

diusulkan oleh Marsh tidak menangani pengumpulan rekomendasi yang diberikan oleh agen lain, Marsh hanya mencontohkan kepercayaan langsung antara dua agen.

Penelitian terhadap Model Kepercayaan

Penelitian terhadap model kepercayaan telah dilakukan oleh peneliti-peneliti sebelumnya. Penelitian yang dilakukan Arabsorkhi, A., Haghighi, M., dan Ghorbanloo, R. pada tahun 2016 [5] dengan model kepercayaan konseptual untuk interaksi *internet of things* dengan memodelkan kepercayaan antara benda/objek, mempelajari model kepercayaan dan menemukan bagaimana objek dapat saling mempercayai.

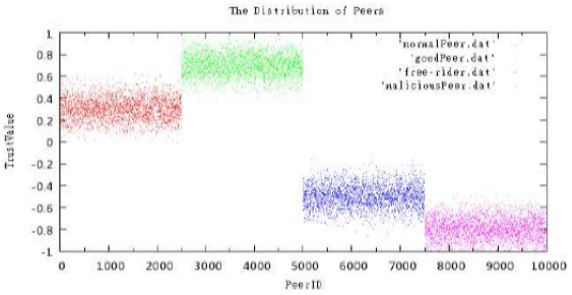
Model kepercayaan IoT harus mengumpulkan informasi tentang kandidat yang ingin mendapat layanan atau memberikan layanan. Jika ada banyak kandidat, harus ada mekanisme pemeringkatan untuk memprioritaskannya. Setelah entitas dipilih dan transaksi terjadi, maka harus memperbarui database sesuai dengan pengalaman dan hukuman/hadiah penghargaan kepada penyedia layanan, baik secara lokal di database-nya atau secara global di jaringan.

Kemudian, Christianson, B., Sidhu, N. dan Xiao, H., pada tahun 2015 [6] melakukan penelitian terhadap penjaminan dan model kepercayaan berbasis reputasi untuk *social internet of things*. Model kepercayaan dilakukan dengan uji simulasi menggunakan arsitektur berdasarkan skenario dunia nyata. Tujuan dari model kepercayaan ini adalah untuk melihat seberapa cepat model dapat mengidentifikasi node berbahaya dan mengisolasi dari jaringan. Hasil dari model kepercayaan yang diusulkan dapat membuat skala dengan mudah ke jaringan besar, karena tidak membebani node dengan penghitungan reputasi dan prosedur pencarian jalur. Penggunaan dua parameter (kredit dan reputasi) untuk membangun kepercayaan dan mendeteksi node berbahaya membuat model ini dapat diandalkan. Penggunaan hukuman untuk aktivitas berbahaya memungkinkan model ini mendeteksi dan mengisolasi node berbahaya.

Huang, G., Hu, M., Liu, P., Zhou, Y., dan Zhang, P. pada tahun 2012 [7] melakukan penelitian terhadap model kepercayaan terdistribusi berdasarkan manajemen reputasi *peer* pada layanan VoD $peer - to - peer$. Jaringan $Peer - to - Peer$ (P2P) adalah sekumpulan *peer*, seperti komputer atau perangkat digital, yang menggunakan kapasitas pengunggahan kolektif mereka untuk menyediakan layanan satu sama lain.

Media streaming P2P atau teknologi P2P telah menjadi solusi paling populer untuk aplikasi $Video - on - Demand$ (VoD) skala besar. Namun ada kelemahan dalam jaringan P2P yang harus diselesaikan seperti masalah $free - riding$. *Peers* yang menikmati $free - riding$ berusaha untuk mendapatkan keuntungan dari *peers* lain tanpa memberikan layanan mereka untuk berbagi sebaik mungkin.

Pada penelitian ini, peneliti merancang simulasi model kepercayaan terdistribusi berdasarkan *Hidden Markov Model* (HMM). Eksperimen simulasi diimplementasikan di lingkungan simulasi PeerSim dan untuk memeriksa kinerja *trust model* dibagi kedalam berbagai skenario. *Peer* dibagi menjadi dua jenis berdasarkan tindakannya: *peer* yang baik (tidak pernah memberikan layanan buruk saat dipilih) dan *peer* yang buruk (mengeksploitasi sumber daya jaringan P2P tanpa berkontribusi ke jaringan P2P VoD pada tingkat yang diinginkan). Gambar 1 adalah nilai kepercayaan eksperimental dari *peer* yang baik dan *peer* yang buruk di jaringan P2P acak dan mereka adalah garis distribusi kabur yang diinginkan eksperimen.



Gambar 1: Distribusi Nilai Kepercayaan Peer di Jaringan P2P Acak.

Dalam percobaan, 50% node ditetapkan sebagai node buruk dan 50% node ditetapkan sebagai node baik. Simulasi yang dilakukan dapat mengurangi $free - riders$ dalam jaringan P2P VoD dengan nilai reputasi rata-rata node normal sekitar 0,3, nilai reputasi rata-rata peer yang baik sekitar 0,7, nilai reputasi rata-rata $free - riding$ adalah -0,5 dan nilai reputasi rata-rata peer yang jahat adalah -0,8 menggunakan tiga model percobaan, yaitu *trust model* yang dirancang, model $tit - for - tat$ di BitTorrent dan model acak.

Model Kepercayaan pada Jejaring Sosial

Manusia sebagai makhluk sosial butuh untuk terus melakukan interaksi, meski harus dilakukan dalam keadaan berjarak sekalipun. Hal ini menghadirkan berbagai situs jejaring sosial, seperti Twitter, Facebook, Instagram, dan lainnya.

Jejaring sosial merupakan sebuah bentuk layanan internet yang ditunjukkan sebagai komunitas *online* bagi orang yang memiliki kesamaan aktivitas, ketertarikan pada bidang tertentu, atau kesamaan latar belakang tertentu. Istilah jejaring sosial diperkenalkan pada tahun 1954 oleh Prof. J.A. Bames, yang mendefinisikan bahwa jejaring sosial adalah struktur sosial yang terdiri dari elemen-elemen individual atau organisasi [8].

Kemajuan teknologi sekarang, menjadikan situs jejaring sosial tidak hanya bisa diakses melalui perangkat komputer. Tetapi juga tersedia dalam bentuk aplikasi yang bisa diunduh dan dipasang pada perangkat seluler. Berbagai kemudahan yang tersedia dalam situs jejaring sosial, tidak memberikan jaminan terhadap kebenaran dari setiap informasi yang ada. Tidak jarang ditemukannya informasi bohong atau palsu. Karenanya, model kepercayaan dibutuhkan dalam penggunaan jejaring sosial.

Penelitian terhadap Model Kepercayaan pada Jejaring Sosial

Penelitian terdahulu terkait model kepercayaan pada jejaring sosial telah dilakukan. Penelitian oleh Cai, Z., Gao, Y., Han, Q., Tong, X., Wang, Y., dan Yin, G. pada tahun 2016 [9] melakukan penelitian terhadap pengukuran model kepercayaan berbasis teori permainan untuk jejaring sosial. Tingkat kepercayaan dihitung dari tiga aspek yaitu, kehandalan pelayanan, efektivitas umpan balik dan kredibilitas rekomendasi.

Untuk mengatasi masalah tumpangan bebas, menggunakan mekanisme hukuman berbasis teori permainan untuk kepercayaan khusus dan kepercayaan global. Hasil dari simulasi awal menunjukkan terdapat masalah $free-riding$ serta proporsi node yang sepenuhnya berbahaya dan node berbahaya acak terus meningkat dalam 50 simulasi awal. Ini diatasi dengan memberikan mekanisme hukuman agar node berbahaya tidak mendominasi arah evolusi seluruh jaringan. Setelah mekanisme hukuman ditambahkan, node terpercaya sepenuhnya dapat mendominasi arah evolusi seluruh jaringan dan hanya node terpercaya seluruhnya jugalah yang dapat bertahan. Masalah ini diatasi dengan menyesuaikan kekuatan mekanisme hukuman untuk menghindari masalah *cold boot*. Setelahnya, proporsi tiap node meningkat dan cenderung stabil.

Masih ditahun 2016, Bundi Ntwiga, D., Weke, P. and Kiura Kirumbu, M. [10] melakukan penelitian untuk model kepercayaan terhadap jejaring sosial menggunakan *Singular Value Decomposition* (SVD) untuk memperkirakan dan mengekstrak tingkat kepercayaan dari matriks nilai nyata.

Tabel 1: Perbandingan uji Friedman antara Trust, Reputation dan Noise

Error term (%)	10	20	30	40	50	60	70
Reputa-tion & Trust	0,0184	0,1573	0,2513	0,1573	0,1083	0, 1573	0, 1573
Trust & Noise	0,0073	0,1083	0,2513	0,1573	0, 1083	0, 1573	0,2513
Reputa-tion & Noise	0,0073	0,1083	0,1573	0,1573	0,1573	0, 1573	0,2513

Tabel 1 merupakan hasil uji Friedman untuk tujuh nilai pertama dari suku kesalahan$\alpha\varepsilon$[0,1; 0,7]. Pada α=0,1 pengujian signifikan secara statistik yang menunjukkan bahwa dalam mengestimasi kepercayaan dari reputasi, terdapat komponen kebisingan. Padaα=0,2 ke atas, tes tersebut tidak signifikan secara statistik. Ini menunjukkan bahwa hanya dapat mengurangi peringkat reputasi dengan istilah kesalahan 20% untuk mencapai hasil yang diinginkan dalam memperkirakan kepercayaan dari peringkat reputasi.

Meningkatkan istilah kesalahan di atas 30% tidak meningkatkan kinerja model. Jadi, 20% adalah tingkat optimal untuk mendiskontokan peringkat reputasi untuk memperkirakan nilai kepercayaan agen di jejaring sosial. Secara umum, terdapat kesamaan yang tinggi antara kepercayaan dan reputasi. Oleh karena itu, peringkat reputasi merupakan faktor penting dalam memperkirakan kepercayaan dan peringkat ini adalah nilai kepercayaan yang diharapkan secara akurat.

Selanjutnya, Chatterjee, M., dan Davoudi, A. ditahun 2016 [11] melakukan penelitian terhadap model kepercayaan untuk memprediksi peringkat produk di jejaring sosial. Model kepercayaannya adalah model kepercayaan sosial menggunakan metode faktorisasi matriks probabilistik untuk memperkirakan selera pengguna dengan memasukkan matriks peringkat item pengguna.

Pengaruh selera pengguna dimodelkan menggunakan model kepercayaan yang didefinisikan berdasarkan kepentingan (sentralitas) dan kesamaan antar pengguna. Kesamaan dimodelkan menggunakan algoritma *Vector Space Similarity* (VSS) dan sentralitas dihitung menggunakan dua ukuran sentralitas yang berbeda (derajat dan sentralitas eigen-vektor). Validasi metode yang diusulkan untuk estimasi peringkat dilakukan pada dataset Epinions.

Epinions adalah situs review dan rating yang memungkinkan pengguna untuk menilai item dengan memberikan bilangan bulat antara 1 dan 5. Model kepercayaan disajikan sebagai penjumlahan linear dari sentralitas dan kesamaan menggunakan faktor pembobotan β.

Opini pengguna tentang produk tertentu akan menjadi fungsi linier dari rasa koneksinya dan seleranya sendiri yang ditentukan oleh faktor pembobotan α. Hasil dari penelitian menunjukkan model kepercayaan yang diusulkan berkinerja lebih baik dibandingkan dengan kepercayaan biner untuk nilai α yang berbeda. Di antara dua ukuran sentralitas, sentralitas derajat memiliki nilai MAE yang lebih rendah yaitu senilai 0.8195. Hasil nilai MAE dapat dilihat pada Tabel 2.

Tabel 2: Nilai MAE untuk model kepercayaan yang berbeda

Trust Model	MAE (80 percent)
Binary	0.8214
Degree Cent.	0.8195
EV Cent.	0.8213

Model kepercayaan yang diusulkan menggunakan algoritma *Vector Space Similarity* (VSS) kepentingan dimodelkan oleh sentralitas derajat dan sentralitas vektor eigen menunjukan hasil yang lebih baik dan akurat dibandingkan dengan hanya menggunakan kepercayaan biner.

Chang-Tien Lu, Chen I., Hua, T., dan Zhao, L. pada tahun 2015 [12] melakukan penelitian yang topiknya berfokus pada model kepercayaan untuk Twitter. Twitter sebagai salah satu alat perpesanan sosial paling popular, menjadi sumber informasi yang menjanjikan untuk mendapatkan pengetahuan dan berita terkini di sekitar.

Peneliti mengusulkan metode baru untuk memperkirakan kepercayaan pengguna/data di Twitter. Metode yang diusulkan pertama-tama secara akurat mengidentifikasi tweet terpercaya yang berfokus pada topik, dan kemudian memperbarui kepercayaan pengguna/data melalui penyebaran kepercayaan berulang. Untuk mengatasi masalah skalabilitas, peneliti menerapkan metode evaluasi kepercayaan berbasis kesamaan dengan properti heterogen kontekstual untuk menilai pengguna/tweet terhadap pengguna/tweet yang dapat dipercaya (misalnya dari pihak berwenang) tanpa perlu upaya manusia dalam memberi label tweet yang kredibel untuk pembelajaran yang diawasi. Eksperimen pada deteksi acara Twitter menunjukkan bahwa metode yang diusulkan dapat secara efektif mengekstrak tweet yang dapat dipercaya sambil mengecualikan rumor dan kebisingan. Hasil perbandingan metode yang diusulkan dengan skema baseline, dapat dilihat pada Tabel 3.

Tabel 3: Perbandingan Kinerja Kuantitatif dari Metode yang Diusulkan dengan Skema Baseline dalam Skor Kepercayaan dan Relevansi dari Tweet yang Diekstraksi

Country	Baseline			Model yang Diusulkan		
	Trust (%)	Relev. (%)	Amount	Trust (%)	Relev. (%)	Amount
Argen-tina	67	71	1836	69	82	1839
Brazil	62	76	577	80	76	2102
Chile	66	70	1803	75	65	1714
Colombia	70	82	1820	83	85	2542
Ecuador	65	68	366	69	65	242
El Salvador	56	68	146	72	70	110
Mexico	71	85	3109	78	91	2349
Paraguay	83	70	136	68	68	202
Uruguay	71	68	139	67	70	124
Venezuela	75	78	4702	91	89	5404
Total	**71**	**78**	**14634**	**82**	**83**	**16629**

Selain itu, analisis kinerja komparatif menunjukkan bahwa metode yang diusulkan mengungguli skema pembelajaran terawasi yang ada menggunakan *tweet* yang diberi label secara manual atau *tweet* yang dihasilkan berdasarkan pencocokan kata kunci sebagai rangkaian pelatihan. Penelitian ini mengasumsikan perilaku serangan persisten, yaitu, serangan pengguna jahat tanpa penyamaran setiap kali ada kesempatan.

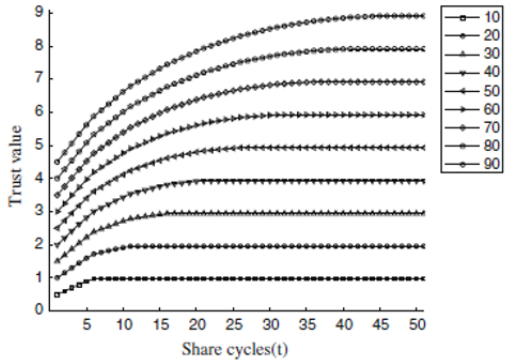
Pada tahun 2013, Bista, S., Nepal, S., Paris, C., dan Sherchan, W. [13] melakukan penelitian terhadap model kepercayaan untuk analisis jejaring sosial menggunakan model Strust, sebuah model kepercayaan sosial yang memperkenalkan konsep kepercayaan keterlibatan dan menggabungkannya dengan kepercayaan popularitas untuk mendapatkan kepercayaan sosial dari komunitas serta anggota individu dalam komunitas. Dilakukan beberapa eksperimen menggunakan kumpulan data nyata yang mewakili jejaring sosial mirip Facebook. Kumpulan data tersebut dapat dilihat pada Tabel 4.

Tabel 4: Dataset eksperimen

Facebook like Social Network	Private Messages Data-Dataset I	Forum Interaction Data-Dataset II
Total number of members	1899	899
Total number of interactions	59835	1113924
Number of unique interactions	20296	142760

Tujuan pemilihan dataset dengan karakteristik yang berbeda adalah untuk mengamati model dalam pengaturan yang berbeda. Hasil dari analisis model yang diusulkan menunjukkan bahwa modal sosial jaringan menurun lebih dari 50% ketika 5% dari anggota yang sangat tepercaya dan interaksinya dihilangkan dari komunitas. Tetapi naik menjadi 80% ketika 15% dieliminasi. Analisis model yang diusulkan juga memberikan wawasan bahwa perbedaan persentase antara total interaksi dan interaksi unik lebih tinggi di komunitas yang sangat interaktif dibandingkan dengan komunitas dengan jumlah interaksi lebih rendah.

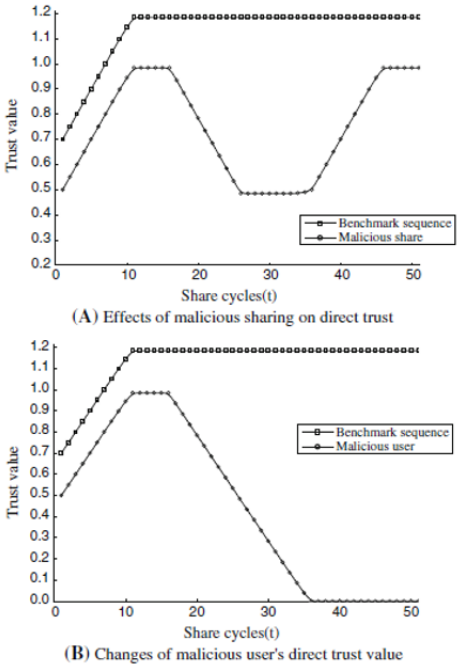
Kemudian Wang, K. dan Zhang, Z. pada tahun 2013 [14] melakukan penelitian terhadap model kepercayaan untuk jejaring sosial multimedia menggunakan metode yang diberi nama *Multimedia Sosial Network Trust Model* (MSNTM). Metode ini berdasarkan teori dunia kecil dan untuk melakukan eksperimen simulasi untuk memverifikasi keefektifan model yang digunakan.



Gambar 2: Dampak ukuran jendela pada kepercayaan langsung

Model kepercayaan MSNTM mencakup model kepercayaan langsung dan model kepercayaan rekomendasi. Gambar 2 menunjukkan dampak panjang jendela pada pembentukan hubungan kepercayaan langsung. Angka tersebut mengakumulasi urutan nilai kepercayaan dalam jendela panjang yang berbeda, dan membuat gerakan paralel ke satu unit untuk memudahkan diferensiasi dan pengamatan.

Hasil dari eksperimen simulasi berdasarkan Gambar 2 menunjukan bahwa nilai kepercayaan langsung adalah proses yang terakumulasi, dan lamanya kontak interaksi secara langsung berdampak pada kecepatan membangun kepercayaan langsung. Gambar 3 mengilustrasikan dampak dari berbagi berbahaya pada nilai kepercayaan langsung.

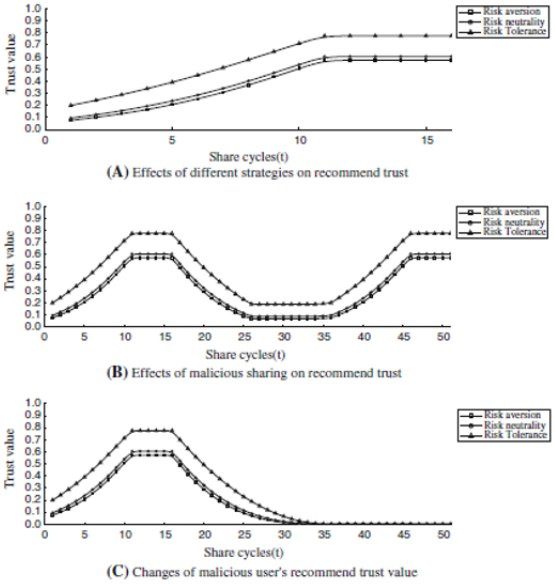


Gambar 3: Eksperimen simulasi kontras kepercayaan langsung

Pada Gambar 3a, nilai kepercayaan menunjukkan tren turun yang jelas dibandingkan dengan urutan kepercayaan dasar setelah sejumlah kecil sesi berbagi berbahaya ditambahkan. Saat pengguna membuat sesi berbagi normal lagi, nilai kepercayaan tidak segera meningkat.

Gambar 3b mengilustrasikan bahwa ketika pengguna berbagi berbahaya membuat banyak sesi berbagi berbahaya, nilai kepercayaan mereka berkurang secara bertahap hingga ditutup pada 0. Hasil eksperimen simulasi juga menunjukan bahwa nilai kepercayaan rekomendasi yang diperoleh berada pada level yang lebih rendah dibandingkan dengan nilai kepercayaan langsung.

Model MSNTM sensitif tehadap bagian berbahaya dari interaksi di jejaring sosial yang membawa dampak hukuman tertentu sehingga memboikot perilaku berbagi yang berbahaya dan mempromosikan konten digital yang normal dan aman, atau pembagian hak di antara pengguna. Sedangkan, Gambar 4 mengilustrasikan dampak kontras rekomendasi kepercayaan.



Gambar 4: Eksperimen simulasi kontras rekomendasi kepercayaan

Gambar 4a menunjukkan bahwa nilai kepercayaan rekomendasi yang diperoleh dari tiga jenis strategi sintetik rekomendasi kepercayaan berada pada level yang lebih rendah dibandingkan dengan nilai kepercayaan langsung. Gambar 4b mengilustrasikan bahwa sesi berbagi berbahaya yang ditambahkan dalam siklus berbagi dengan cepat menurunkan kepercayaan pada tiga jenis strategi sintetis. Gambar 4c menunjukkan bahwa terlalu banyak berbagi berbahaya dalam siklus berbagi dengan cepat menurunkan nilai kepercayaan ke 0.

Eksperimen simulasi juga menunjukkan bahwa MSNTM dapat secara dinamis memperbarui nilai kepercayaan antara pengguna secara *real time*. Ini menyesuaikan skenario berbagi konten digital dalam berbagai jenis risiko. Mekanisme jendela kalkulasi kepercayaan dapat mengevaluasi secara akurat dan secara dinamis memperbarui hubungan kepercayaan antar pengguna.

Similarity

Similarity dalam bahasa inggris memiliki arti kesamaan, kemiripan, persamaan, dan/atau keserupaan. *Similarity* dalam kata adalah mencari kesamaan antara kata masukkan (*input*) dengan kata sumber. Kesamaan kata yang dimaksud adalah kata yang paling mendekati kata sebenarnya. Contohnya pada penggunaan kata "jgn" yang memiliki kesamaan kata atau kata sebenarnya dari kata "jangan".

Salah satu fungsi *similarity* adalah sebagai *key tape error correction* atau koreksi kesalahan pengetikkan. Fungsi lainnya adalah untuk mengetahui kesamaan antara dua kata yang saling berkecocokan.

Ketika melakukan pencarian materi tertentu, seperti artikel, ulasan, atau makalah, kesamaan dengan materi satu dengan materi yang lainnya mungkin muncul. Namun, ini bukan berarti bahwa konten yang bersangkutan telah dijiplak. Karena, biasanya suatu materi bisa mengutip beberapa judul makalah lain yang terdeteksi sebagai kesamaan. Berikut dengan nama, judul buku atau bibliografi, referensi dan kutipan, frasa, dan konstruksi umum. Sehingga tidak bisa dikatakan sebagai jiplak karena tidak memenuhi syarat sebagai plagiarism, yang menyiratkan penggunaan karya atau ide orang lain seolah-olah milik sendiri [15].

Similarity sebagai Model Kepercayaan

Penggunaan metode *similarity* untuk model kepercayaan telah banyak dilakukan oleh para peneliti. Hubungan virtual dibangun di atas metrik yang digunakan untuk menghubungkan pengguna berdasarkan pengalaman mereka dan disebut dengan kesamaan [16]. Sederhananya, setiap kesamaan yang muncul dan ada dari setiap pengguna, akan menimbulkan kepercayaan diantara mereka.

Berbagai metrik kesamaan telah diterapkan dalam skenario yang berbeda, seperti model kepercayaan yang didasarkan pada kesamaan konten transaksi $e-commerce$ dan membedakan tingkat kepercayaan rekomendasi node kenalan dari rekomendasi node asing (TCSRTrust) [17]. Kemudian juga model kepercayaan dengan mekanisme deteksi hubungan kepercayaan dari jejaring sosial egosentris untuk menghitung tingkat kepercayaan antara pengguna aktif dan teman-temannya yang diarahkan dengan model yang disebut LoTrust. Model komputasi ini didasarkan pada metrik kepercayaan baru yang didasarkan tidak hanya pada kesamaan minat pengguna menurut profil sosial semantik mereka (RDF/FOAF), tetapi juga memperhitungkan faktor waktu interaksi aktif pengguna [18].

Penelitian terhadap Similarity

Penelitian terhadap *similarity* telah dilakukan oleh peneliti-peneliti sebelumnya. Penelitian oleh Arief, R., Pratama, Z., dan Utami, E. [19] pada 2019 melakukan perbandingan jenis n-gram dalam penentuan *similarity* pada deteksi plagiat.

N-gram adalah model *probabilistic* yang awalnya dirancang oleh ahli matematika dari Rusia pada awal abad ke-20, dan kemudian dikembangkan untuk memprediksi item berikutnya dalam urutan item. Penelitian ini juga menggunakan algoritma Rabin-Karp yang ditemukan oleh Michael O. Rabin dan Richard M. Karp. Peneliti menggunakan softcopy skripsi sebagai bahan uji untuk penentuan similarity deteksi plagiat. Proses pengujian dilakukan dengan memilih dokumen asal, kemudian memilih dokumen target terhadap 6-gram char, 6-gram word, oneskipgram, dan dotskipgram. Hasil pengujian yang telah didapatkan dapat untuk dilanjutkan ke proses untuk melakukan analisa perbandingan terhadap masing-masing jenis n-gram.

Tabel 5: Hasil Pengujian Perbandingan Ketepatan Jenis N-Gram

No.	Pengujian Dok.	Ketepatan – Selisih Similarity (%)			
		n-gram char	n-gram word	one-skip-gram	dot-skip-gram
1	Dok1 → Dok2	23	3	4	6
2	Dok1 → Dok3	10	2	27	28
3	Dok1 → Dok4	0	14	28	31
4	Dok2 → Dok3	5	0	24	26
5	Dok2 → Dok4	15	1	7	6
6	Dok3 → Dok4	13	9	12	13

Tabel 5 menyajikan perbandingan ketepatan hasil penghitungan *similarity* dari instrumen uji. Ketepatan merupakan selisih persentase *similarity* dari instrumen dengan *similarity* dari *software* Plagiarism Checker X Free. Sehingga definisi ketepatan dalam perbandingan ini adalah nilai *similarity* hasil dari instrumen yang bernilai paling kecil (selisih paling kecil di antara keempat fungsi n-gram). Selain membandingkan ketepatan, juga melakukan perbandingan kecepatan.

Kecepatan diperoleh dari penghitungan selisih CPU *tick* yang didapatkan sebelum fungsi dijalankan dan saat fungsi berhasil mendapatkan nilai atau selesai melakukan eksekusi perintah. Berikut Tabel 6 yang menyajikan perbandingan kecepatan eksekusi fungsi n-gram.

Tabel 6: Hasil Pengujian Perbandingan Kecepatan Jenis N-Gram

No.	Pengujian Dok.	Kecepatan (s)			
		n-gram char	n-gram word	one-skip-gram	dot-skip-gram
1	Dok1 → Dok2	1,34	0,41	0,52	0,35
2	Dok1 → Dok3	1,25	0,34	0,43	0,33
3	Dok1 → Dok4	1,26	0,34	0,36	0,38
4	Dok2 → Dok3	1,88	0,54	0,59	0,55
5	Dok2 → Dok4	1,68	0,47	0,51	0,44
6	Dok3 → Dok4	2,00	0,65	0,62	0,53

Hasil dari pengujian ini adalah, dari keempat tipe n-gram menunjukan jika n-gram *word* memiliki ketepatan akurasi yang paling baik, pengujian kecepatan waktu proses menunjukkan jika $dot-skip-gram$ yang paling cepat, kemudian diikuti oleh n-gram word.

Berikutnya, Faisal, M., Hanani, A. Pratama, dan Putriwana, R. [20] melakukan penelitian pada tahun 2019 dengan melakukan deteksi *plagiarism* pada artikel jurnal menggunakan metode *cosine*

similarity. *Cosine similarity* adalah metode perhitungan antara dua buah dokumen yang bertujuan untuk mengetahui tinkat kemiripan antar dokumen tersebut.

Perhitungan metode *cosine similarity* didasarkan pada dua buah vektor yang memiliki kemiripan jumlah kata pada dua dokumen yang dibandingkan. Metode cosine similarity mempunyai konsep normalisasi panjang vektor data dengan membandingkan N-gram yang sejajar satu dengan lainnya dari 2 pembanding.

Peneliti mengumpulkan data berupa jurnal *online* melalui berbagai website. Hasil dari penelitian ini adalah nilai akurasi sistem dengan melakukan perhitungan *recall* dan *precision* dari perhitungan *cosine* dengan mengambil data dan membandingkan dengan *repository* yang telah ada. Nilai recall untuk kasus ini yaitu 13%, diperoleh dari jumlah dokumen relevan yang terambil dibagi dengan jumlah dokumen yang ada dalam database dikali 100%. Sedangkan nilai *precision* yaitu 8%, diperoleh dari jumlah dokumen relevan yang terambil dibagi dengan jumlah dokumen relevan yang ada dalam pencarian dikali 100%.

Adeel Nawab, Pervaz, I., dan Shahzad, K. [21] pada tahun 2018 melakukan penelitian tentang ukuran *semantic similarity* berbasis WordNet untuk pencocokan model proses. WordNet secara luas diakui sebagai sumber yang berharga untuk menemukan kesamaan *semantic* antara dua kata karena mengatur kata-kata berdasarkan hubungan leksikal dan kemudian mendefinisikan hubungan *semantic* antara *synsets* yang terkait secara leksikal tersebut. Pada penelitian ini, digunakan tiga kumpulan data yang dikembangkan oleh para ahli dan digunakan dalam kontes PMMC tahun 2015. Spesifikasi dari ketiga dataset diberikan di bawah ini pada Tabel 7.

Tabel 7: Spesifikasi Kumpulan Data PMMC'15

	UA Dataset	BR Dataset	AM Dataset
Jumlah Kegiatan (Min)	12	9	1
Jumlah Kegiatan (Max)	45	25	43
Jumlah Kegiatan (Avg)	24,2	17,9	18,6
Jumlah Korespodensi 1:1	268	156	140
Jumlah Korespodensi 1:n	360	427	82

Tujuan utama penelitian ini adalah untuk mengklasifikan setiap pasangan aktivitas sebagai 'setara' atau 'tidak setara'. Karena metode *semantic similarity* yang digunakan mengembalikan skor *numeric* antara 0 (tidak setara) dan 1 (setara) pada sembilan ambang batas yang berbeda dari 0,1 hingga 0,9 dengan celah 0,1. Namun pada penelitian ini, peneliti menggunakan ambang batas 0,7. Nilai ambang batas ini menyatakan bahwa setiap pasangan aktivitas yang skor kesamaannya lebih besar atau sama dengan 0,7 ditandai sebagai setara (atau 1) dan tidak setara (atau 0) sebaliknya. Hasil dari semua teknik yang digunakan untuk dataset PMMC'15 dapat dilihat pada Tabel 8.

Tabel 8: Hasil dari Semua Teknik untuk Dataset PMMC'15

Level Kalimat	Word-level	UA Dataset	BR Dataset	AM Dataset
Greedy Pairs	Resnik	**0,516**	0,532	**0,464**
	Jiang	**0,516**	**0,534**	**0,464**
	Leacock	0,487	0,509	0,453
	Lin	0,513	0,533	0,453
	Wu	0,495	0,516	0,456
Optimal Pairing	Resnik	0,519	0,532	**0,464**
	Jiang	0,516	**0,534**	**0,464**
	Leacock	0,489	0,516	0,454
	Lin	**0,520**	0,533	0,456
	Wu	0,495	0,525	0,457
QAP	Resnik	0,520	0,532	**0,464**
	Jiang	0,520	**0,534**	**0,464**
	Leacock	0,498	0,522	0,455
	Lin	**0,525**	**0,534**	0,457
	Wu	0,508	0,525	0,459

Hasil dari Tabel 8, dapat diambil beberapa analisis singkat yaitu: 1) terdapat perbedaan untuk tingkat kesulitan dari dataset yang ditandai dengan perbedaan performansi disetiap teknik yang digunakan, 2) terdapat variasi kinerja diseluruh ukuran tingkat kata, dan 3) terdapat variasi kinerja diseluruh metode tingkat kalimat.

Hasil penelitian menunjukkan sebagai berikut: a) kekerasan ketiga dataset berbeda, dengan dataset AM yang paling sulit, dataset BR menjadi yang paling moderat, dan dataset UA yang paling mudah, b) Jiang similarity, adalah teknik pencocokan yang paling cocok, dan c) Pairing QAP adalah ukuran tingkat kalimat yang paling efektif. Untuk pengerjaan di masa depan, peneliti mengusulkan untuk membandingkan kinerja ukuran semantic dengan semua teknik pencocokan yang ada.

Penutup

Berbagai penelitian terhadap model kepercayaan telah banyak dilakukan oleh para peneliti. Menandakan bahwa kepercayaan memiliki peran yang sangat penting dalam berinteraksi dikehidupan sehari-hari, terlebih interaksi yang dilakukan melalui dunia maya atau internet.

Model kepercayaan terhadap dunia maya, khususnya melalui jejaring sosial juga telah banyak dilakukan oleh para peneliti. Guna untuk mengetahui dan mengukur kepercayaan pengguna ter-

hadap pengguna lain dalam berinteraksi di jejaring sosial. Hasil yang didapatkan pun beragam, bergantung pada ruang lingkup pengujian dan faktor yang memengaruhinya. Sebagian besar menunjukan bahwa, kepercayaan membawa pengaruh pada tindak perilaku pengguna terhadap suatu kejadian atau suatu konten yang tersebar di jejaring sosial.

Penggunaan metode *simalirity* dapat menjadi opsi lanjutan dalam mengimplementasikan model kepercayaan kedepannya. *Similarity* yang berarti kesamaan, menjadi dasar untuk terbentuknya suatu kepercayaan. Jika memiliki kesamaan, manusia cenderung untuk percaya terhadap hal tersebut.

Daftar Pustaka

[1] D. Andert, R. Wakefield and J. Weise, "Trust Modelling for Security Architecture Development", Journal of Sun Microsystems BluePrints, 2002.

[2] S. Singh and S. Bawa, "A Privacy, Trust and Policy based Authorization Framework for Services in Distributed Environtment", International Journal of Computer Science, 2(2), pp: 85-92, 2007.

[3] D. McKnight and N. Chervany, "The Meanings of Trust", Minneapolis, Minn, Carlson School of Management, University of Minnesota, 1996.

[4] S. P. Marsh, "Formalising Trust as A Computational Concept", University of Stirling, Scotland, UK, 1994.

[5] A. Arabsorkhi, M. Haghighi and R. Ghorbanloo, "A Conceptual Trust Model for the Internet of Things Interactions", 2016 8th International Symposium on Telecomunications (IST), 89-93, 2016.

[6] H. Xiao, N. Sidhu and B Christianson, "Guarantor and Reputation Based Trust Model for Social Internet of Things", 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), 600-605, 2015.

[7] G. Huang, M. Hu, Y. Zhou, P. Liu and P. Zhang, "A Distributed Trust Model Based on Reputations Management of Peers for P2P VoD Services", KSII Transactions on Internet and Information Systems, DOI:10.3837/tiis.2012.09.018, 2012.

[8] F. Welta, "Perancangan Social Networking sebagai Media Informasi bagi Pemerintah", Prodising PESAT, ISSN: 1858-2559, vol. 5, 2013.

[9] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong and Q. Han, "A Game Theory-Based Trust Measurement Model for Social Networks", Computational Social Networks, Springer, 3(1), 2, 2016.

[10] D. Bundi Ntwiga, P. Weke and M. Kiura Kirumbu, "Trust Model for Social Network using Singular Value Decomposition", Interdisciplinary Description of Complex Systems: INDECS, Hrvatsko interdisciplinarno društvo, ISSN: 2229-5046, Vol. 14, No. 3, 296-302, 2016.

[11] A. Davoudi and M. Chatterjee, "Product Rating Prediction using Trust Relationships in Social Network", InProceedings 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Electronic ISBN: 978-1-4673-9292-1, Electronic ISSN: 2331-9869, pp. 115-118, 2016.

[12] L. Zhao, T. Hua, , Chang-Tien Lu and I. Chen , "A Topic-focused Trust Model for Twitter", Computer Communications 14(000):38-1, 2015.

[13] S. Nepal, C. Paris, S. Bista, and W. Sherchan, "A Trust Model-Based Analysis of Social Networks", International Journal of Trust Management in Computing and Communications 19, Inderscience Publisher Lts, 1, 3-22, 2013.

[14] Z. Zhang and K. Wang, "A Trust Model for Multimedia Social Networks", Social Network Analysis and Mining, Springer, 3(4), 969-979, 2013.

[15] Anonymous, "Telling The Difference Between Plagiarism and Similarity", diakses daring pada http://blog.checkforplagiarism.net/telling-the-difference-between-plagiarism-and-similarity/, 04 Juni 2021.

[16] Georgios K. Pitslis and L. Marshall, "Modelling Trust for Recommender Systems using Similarity Metrics", IFIP International Conference on Trust Management, Volume 263, pp.103-118, 2008.

[17] G. Wang, X. Gui and G. Wei, "A Recommendation Trust Model Based on E-Commerce Transaction Content-Similarity", 2010 International Conference on Machine Vision and Human-machine Interface, Electronic ISBN: 978-1-4244-6596-5, 2010.

[18] A. Kalaï, A. Wafa, C. Amel Zayan and I. Amous, "LoTrust: A Social Trust Level Model Based on Time-Aware Social Interactions and Interests Similarity", 2016 14th Annual Conference on Privacy, Security and Trust (PST), Electronic ISBN: 978-1-5090-4379-8, 2016.

[19] Z. Pratama, E. Utam dan R. Arief, "Analisa Perbandingan Jenis N-Gram dalam Penentuan Similarity Text pada Deteksi Plagiat", Creative Information Technology Journal, ISSN: 2460-4259, 2019.

[20] R. Pratama Putriwana, M. Faisa dan A. Hanani, "Deteksi Plagiat pada Artikel Jurnal Menggunakan Metode Cosine Similarity", SMARTICS Journal, Vol. 5 No. 1, p22-26, ISSN online: 2474-9754, ISSN print: 2623-0429, 2019.

[21] K. Shahzad, I. Pervaz and Adeel Nawab, "WordNet-based Semantic Similarity Measure for Process Model Matching", 17th International Conference on Perspectives in Business Informatics Research, 2018.