JIUBJ

Jurnal Ilmiah Universitas Batanghari Jambi, 22(2), Juli 2022, 1296-1298
Lembaga Penelitian dan Pengabdian kepada Masyarakat universitas Batanghari Jambi
ISSN 1411-8939 (Online), ISSN 2549-4236 (Print)
DOI 10.33087/jiubj.v22i2.2068

Rancang Bangun Sistem Rekening Bersama untuk Keamanan Transaksi Online dengan Metode *Brute Force String Matching*

Sativa Wahyu Priyanto*, Fatkhul Amin
Universitas Stikubank Semarang
*Correspondence email: sativa.wahyu04@gmail.com, fatkhulamin@edu.unisbank.ac.id

Abstrak. Perkembangan internet yang semakin maju membuat kegiatan yang sebelumnya dilakukan secara *offline* dapat dilakukan dengan cara *online*. Salah satunya adalah perdagangan. Perdagangan yang dilakukan secara online dapat mencakup ruang lingkup yang luas dan bahkan tidak terbatas. Namun melakukan transaksi online tanpa adanya pengaman rawan terjadinya penipuan. Rekening Bersama merupakan konsep transaksi *online* yang aman dengan pihak ke-3 sebagai penengah transaksi. Pencarian kata yang mengandung unsur penipuan dapat meminimalisir terjadinya penipuan. Metode *Brute Force String Matching* merupakan algoritma pencarian kata yang bersifat lurus dan sederhana. Implementasi terhadap sistem rekening bersama dapat mencari secara otomatis kata yang mengandung unsur penipuan. Hasil pencarian kata ditampilkan pada *user* dalam bentuk notif dan sensor sebagian kata.

Kata kunci: Brute Force String Matching; Rekening Bersama; Perdagangan

Abstract. *The development of the internet that is increasingly advanced makes activities that were previously carried out offline can be done online. One of them is trading. Trading conducted online can cover a wide and even unlimited scope. However, making online transactions without security is prone to fraud. Joint Account is the concept of a secure online transaction with a 3rd party as the middleman of the transaction. Searching for words that contain elements of fraud can minimize the occurrence of fraud. The Brute Force String Matching method is a straight and simple word search algorithm. Implementation of the joint account system can automatically search for words that contain elements of fraud. The word search results are displayed to the user in the form of a notification and a partial word sensor.*

Keywords**:** *Brute Force String Matching; Joint Account; Trading*

PENDAHULUAN

Seiring perkembangan teknologi yang semakin pesat dan maju, akses internet semakin mudah dan hampir semua orang mengenal internet, terlebih lagi hampir semua perangkat mendukung layanan internet, seperti halnya smartphone, komputer, dan handphone. Dengan layanan internet, kegiatan yang sebelumnya dilakukan dengan cara *offline* dapat dilakukan secara *online*, salah satunya adalah kegiatan perdagangan. Perdagangan yang dilakukan secara *online* dapat mencakup ruang lingkup yang luas dan bahkan tidak terbatas. Terlebih lagi, proses transaksi *online* dapat dilakukan dimanapun dan kapanpun. Akan tetapi melakukan transaksi *online* yang dilakukan tanpa adanya pihak ketiga mengalami banyak kekurangan, salah satunya adalah tidak adanya sistem pengaman atau validasi, sehingga rawan terjadi penipuan (Cross, 2013).

Sosial Media adalah identitas bagi teknologi digital yang dapat dimanfaatkan orang-orang untuk berinteraksi, memproduksi, berhubungan, serta saling berpesan (Lewis, 2010). Menurut laporan We Are Social, di tahun 2021 terdapat 170 juta pengguna internet di seluruh Indonesia. Dengan pengguna media sosial yang sangat banyak itu, banyak dari mereka yang memanfaatkannya sebagai tempat untuk berdagang. Namun di media sosial memiliki sistem pengaman untuk mengamankan transaksi, sehingga rawan terjadi penipuan. *Marketplace* adalah penyedia media online berbasis *website* tempat terjadinya kegiatan transaksi antara pembeli dan penjual. Pembeli bisa mencari pemasok sebanyak yang diinginkan, sehingga bisa mendapatkan harga seperti pasar (Opiida, 2014). Dengan melakukan transaksi di dalam *marketplace*, keamanan akan lebih terjamin karena *marketplace* memiliki sistem pengaman atau validasi untuk mengamankan transaksi. Selain aman, *marketplace* mendukung banyak metode pembayaran dengan sistem validasi otomatis untuk mempermudah pengguna saat melakukan transaksi. Namun pengguna yang ingin melakukan transaksi secara cepat hanya untuk satu kesepakatan transaksi kurang efektif jika menggunakan *marketplace*, karena proses transaksinya yang membutuhkan waktu yang *relative* lama hanya untuk satu transaksi. Selain itu jika transaksi telah selesai dilakukan, proses pencairan uang yang didapat akan memakan waktu yang *relative* lama, karena sistem marketplace harus melakukan validasi terhadap transaksi yang baru saja diselesaikan.

Sistem rekening Bersama memiliki proses transaksi yang aman dan cepat. Rekening bersama adalah konsep bertransaksi yang aman untuk menghindari terjadinya penipuan (Aditya, 2015). Dalam prakteknya, rekening bersama berperan sebagai penengah antara penjual dan pembeli. Seorang rekber terkadang memberikan biaya untuk jasannya pada setiap transaksi yang nominalnya diputuskan oleh penjual dan rekber. Sistem layanan rekening bersama memiliki

proses transaksi yang berjalan dengan cepat dan jelas, karena seluruh pihak yang terlibat dalam transaksi akan saling berkomunikasi di dalam sistem, sehingga dapat meminimalisir terjadinya miskomunikasi. Rekber bertugas dalam memastikan bahwa barang yang telah dibayar sampai ke penerima, karena kalau tidak, maka uang akan dikembalikan kepada pembeli (Hidayatullah, 2019). Walaupun menggunakan sistem rekening bersama sebagai tempat transaksi, ancaman penipuan masih dapat terjadi karena kelengahan pembeli.

Penelitian ini menggunakan algoritma Brute Force untuk mencari kata yang tidak diperbolehkan saat transaksi sedang berlangsung. Algoritma Brute Force merupakan algoritma yang dapat digunakan untuk. mencocokan *string* dengan teks secara lurus atau *straight forward* (Hajrahnur, 2018). Kata yang tidak diperbolehkan di dalam sistem rekening bersama pada umumnya adalah *URL*, nomor HP, bujukan untuk mengganti metode transaksi, dan kata-kata kotor. Tindakan terhadap kata yang tidak diperbolehkan adalah melakukan pengubahan beberapa kata menjadi simbol bintang dan memberikan notif. Berdasarkan latar belakang di atas, maka penelitian ini mengangkat topik dengan judul "*Rancang Bangun Sistem Rekening Bersama Untuk Mengamankan Transaksi Online Dengan Metode Brute Force String Matching*" (Abdurahman, 2013).

METODE

Algoritma Brute Force

Algoritma Brute Force adalah algoritma dengan sifat lurus atau *straight forward*, yang biasanya disebut sebagai algoritma lempeng (Oktari, 2018). Karena memiliki proses yang lurus untuk menyelesaikan logika, ternyata algoritma Brute Force memiliki masalah pada waktu pemprosesannya yang panjang. Sehingga pada penggunaan algoritma Brute Force dibutuhkan cara penyelesaian yang jelas namun sederhana. Algoritma Brute Force digunakan untuk pencocokan *string*, namun tanpa memikirkan peningkatan performa. Biasanya algoritma ini digunakan untuk studi pembanding dan studi lainnya, sehingga sangat jarang digunakan untuk sebuah sistem. Rumus yang digunakan dalam algoritma Brute Force adalah:

pattern[0..n-1]

teks[0..m-1]

Penjelasan: pattern[0..n-1] merupakan kata yang akan di cocokan pada sebuah *string*, dengan memisahkan setiap huruf sehingga membentuk suatu *array*, selanjutnya pattern tersebut akan di cocokan dengan teks[0..m-1] yang merupakan *string* yang dipisahkan juga setiap hurufnya menjadi *array*. Pencocokan ini akan terus berulang sampai akhir *string*.

Keterangan: n: jumlah huruf; teks: *string* yang akan dicari kata didalamnya; pattern: kata yang dicari.

Secara sistematis, langkah-langkah algoritma Brute Force adalah sebagai berikut:

1. Pattern dan string dipisah per-huruf menjadi *array*.
2. Proses dimulai dari kiri ke kanan, dengan mencocokan setiap hurufnya sampai salah satu kondisi berikut terpenuhi: (a) Huruf yang dicocokan tidak sama; dan (b) semua huruf yang dicocokan sama, yang selanjutnya posisi penemuan akan di simpan ke dalam *variable.*

Proses Algoritma Brute Force akan terus berulang-ulang seperti pada langkah nomor 2, sampai *string* terakhir.

HASIL DAN PEMBAHASAN

Sampel data tersebut berupa kata yang tidak diperbolehkan dan *chat* yang biasanya digunakan untuk membujuk calon korban agar melakukan transaksi diluar rekber/sistem. Penelitian ini mengambil sebanyak dua sampel data kata yang tidak diperbolehkan seperti pada Tabel 1 dan satu chat yang biasanya digunakan untuk membujuk calon korban seperti pada Tabel 2.

Tabel 1. Sampel *Data* Kata Yang Tidak Diperbolehkan

No	Kata Yang Tidak Diperbolehkan
1.	wa
2.	fb

Sumber: data olahan

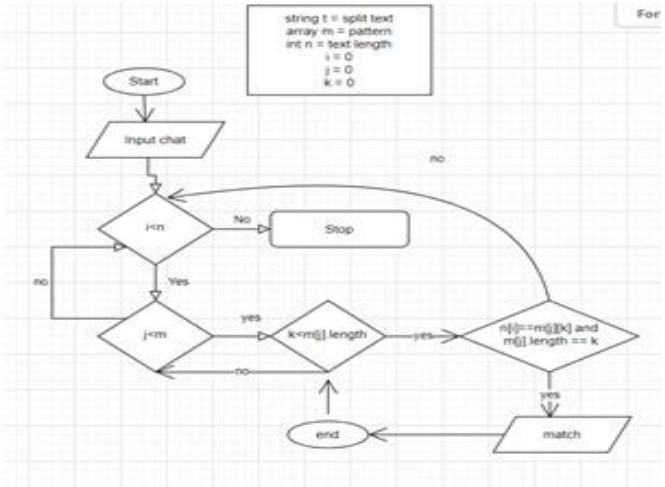
Tabel 2. Sampel *Data Chat* Untuk Menipu

No.	Chat
1.	Transaksi ke fb atau wa

Sumber: data olahan

String Matching

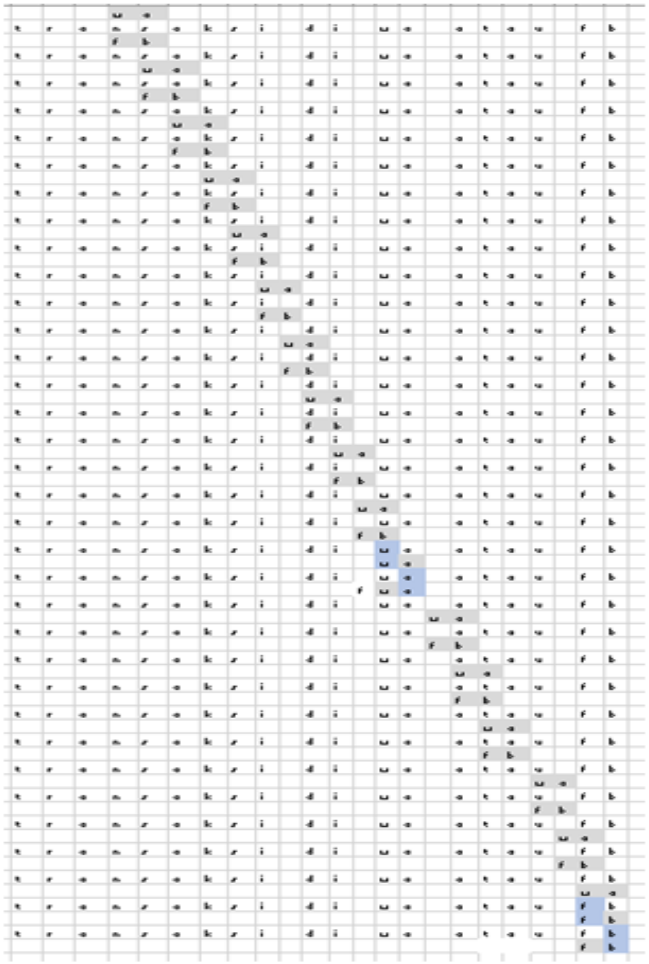
String matching adalah metode untuk mencocokan teks dengan *pattern*. Teks merupakan string dengan Panjang n, sedangkan pattern merupakan string dengan panjang m dimana m < n, yang merupakan pencarian pada teks. Pada gambar 1. Terlihat proses cara kerja flowchart algoritma brute force *string matching* yang mencocokan teks dengan *array pattern*.



Sumber: data olahan

Gambar 1. *Flowchart Brute Force*

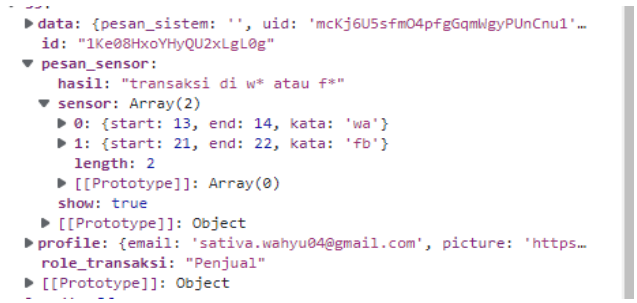
Gambar 2 menjabarkan alur proses pencarian teks dengan pattern dari sampel menggunakan *algoritma Brute Force String Matching*.



Sumber: data olahan

Gambar 2. Alur proses pencarian kata dengan algoritma Brute Force

Proses pencarian kata jika ditemukan kata yang tidak diperbolehkan (*pattern*) pada teks maka proses pencocokan akan langsung berhenti pada kata yang tidak diperbolehkan tersebut, lalu setelah itu proses perulangan akan berjalan kembali terhadap teks pada urutan terakhir ditemukannya kata tidak diperbolehkan ditambah satu. Hal ini dilakukan agar proses pencarian kata lebih cepat dan tidak bertabrakan saat melakukan sensor.



Sumber: data olahan

Gambar 3. JSON hasil pencarian kata

Setelah selesai dilakukannya proses pencarian kata dan sensor sebagian kata pada teks/*chat*, selanjutnya sistem akan menampilkan *chat* tersebut di *frontend*.

Sumber: data olahan

Gambar 4. Tampilan Hasil pencarian kata dan sensor pada sistem

SIMPULAN

Hasil penelitian ini mengungkapkan nahwa hasil pencarian kata ditampilkan pada *user* dalam bentuk notif dan sensor sebagian kata.

DAFTAR PUSTAKA

Lewis, B.K. 2010. Social Media and Strategic Communication : Attitudes and Perceptions Among College Student. *International Journal of Public Relation Society of America*.

Opiida. 2014, *Pengertian E-marketplace*. Retrieved from https://tokohalista.wordpress.com (28 Oktober 2019).

Hidayatullah, M. Syarif., Moch. Nuril Ihsan., Moh. Nur Muhibbin. 2019. *Penggunaan Jasa Rekening Bersama (Rekber) Perspektif Islam*.

Aditya. 2015. *Pengertian Rekber (Rekening Bersama), Cara Kerja dan Manfaatnya*. Diakses pada 30 September 2021, dari https://www.aditya-web.com/2015/03/pengertian-rekber-rekening-bersama-cara-kerja-dan-manfaatnya.html

Cross, Michael. 2013. *Social Media Scurity, 1st Edition: Leveraging Social Network While Mitigating Risk*. Syngress

Hajrahnur, S., Nasrun, M., Setianingsih, C., & Murti, M. A. 2018, Classification of posts Twitter traffic jam the city of Jakarta using algorithm C4. 5. In *2018 International Conference on Signals and Systems (ICSigSys*, 294-300. IEEE.

Abdurahman, D., & Kurniawan, I. 2018, Rancang Bangun Aplikasi Kamus Fisika Dasar Menggunakan Algoritma String Matching Brute Force Berbasis Android. In *Seminar Nasional Teknologi Informasi*, 1, 150-155).

Oktari, U. 2018. Aplikasi Mobile Pencarian Rute Terpendek Pada Pengiriman Order CV. Alfa Fresh dengan Algoritma Brute Force, *Doctoral dissertation*, Politeknik Negeri Sriwijaya.