JNATIA Volume 3, Nomor 2, Februari 2025 p-ISSN: 2986-3929
Jurnal Nasional Teknologi Informasi dan Aplikasinya e-ISSN: 3032-1948

Analisis Keamanan Seed Phrase pada Wallet Cryptocurrency Menggunakan Brute Force

I Kadek Adi Sentana[a1], I Gusti Ngurah Anom Cahyadi Putr**a**[a2]

Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]kadekadi1398@gmail.com
[2]anom.cp@unud.ac.id

Abstract

Cryptocurrency wallets serve as digital repositories for securing various digital assets. The security of these wallets is often bolstered by the utilization of seed phrases, which act as a primary means of access and recovery. This research delves into the examination of wallet security, specifically focusing on assessing the resilience against brute force attacks. Brute force methods entail systematically attempting numerous combinations to crack the seed phrase and gain unauthorized access to the wallet contents. Through meticulous experimentation and analysis, this study aims to provide insights into the effectiveness of seed phrase-based security mechanisms in thwarting brute force intrusion attempts. By evaluating different wallet implementations and their susceptibility to brute force attacks, this research contributes to enhancing the robustness of cryptocurrency wallet security measures.

Keywords: *wallet, security, brute force, seed phrase, cryptocurrency*

1. Pendahuluan

Cryptocurrency merupakan bentuk mata uang digital yang sedang mengalami peningkatan signifikan belakangan ini. Berbeda dengan uang kertas fiat yang umumnya digunakan, cryptocurrency tidak mencatat jejak kepemilikan atau transaksi pengguna. Cryptocurrency ini didasarkan pada dua hal, yaitu blockchain yang berperan sebagai buku besar untuk aset dan transaksi, kemudian kriptografi yang berfungsi sebagai sarana untuk melindungi aset. [3] Pengguna cryptocurrency membutuhkan sebuah wallet sebagai tempat untuk menerima dan mengirim koin dari orang lain sebagai pembayaran atas barang atau jasa yang mereka beli atau jual menggunakan aset cryptocurrency. Wallet ini berfungsi sebagai alat penyimpanan dan manajemen yang memungkinkan pengguna untuk mengelola transaksi mereka dalam ekosistem cryptocurrency. Pada dasarnya, ada tiga jenis wallet cryptocurrency yang bisa digunakan oleh pengguna cryptocurrency, cold wallet yang merupakan wallet perangkat keras, hot wallet merupakan wallet yang dihosting di internet, dan warm wallet yang dapat diunduh di komputer pribadi, laptop, dan perangkat seluler pengguna. [4] Meskipun cryptocurrency memiliki keunggulan seperti biaya transaksi yang rendah, eliminasi biaya bank, dan anonimitas dalam berbelanja, namun juga memiliki kelemahan seperti fluktuasi harga yang tinggi, transaksi yang tidak dapat dikembalikan, serta rentan terhadap serangan seperti time jacking, pembelanjaan ganda, dan penambangan egois. Kekhawatiran serius lainnya adalah resiko kehilangan aset jika seed phrase wallet yang mengelola aset tersebut terlupakan atau hilang. Pada saat ini, terdapat berbagai macam mata uang kripto yang diperdagangkan di pasar dan nilainya terus berubah sesuai dengan permintaan pasar. Terdapat banyak pilihan dompet mata uang kripto yang dapat diakses secara daring, yang memungkinkan pengguna untuk mengelola aset kripto mereka dan melakukan transaksi. Proses pemasangan dan pengaturan dompet pada perangkat komputer atau seluler menghasilkan sebuah seed phrase yang di dalamnya berisi serangkaian 12-24 kata bahasa Inggris yang mewakili entropi dari seed phrase. Ini adalah terjemahan entropi ke dalam format yang mudah dibaca, tetapi mempertahankan informasi yang sama.yang terdiri dari 12 hingga 24 kata, yang disarankan untuk disimpan dengan aman sebagai frasa cadangan atau pemulihan. [2] Penelitian ini akan menguji keamanan sebuah seed phrase dalam sebuah dompet

kripto dengan menggunakan serangan brute force. Frase benih tersebut akan diuji dengan mencoba berbagai kombinasi kata-kata yang sesuai dengan standar BIP 39, yang merupakan daftar kata-kata yang diusulkan untuk menciptakan seed phrase. Tujuan pengujian adalah untuk mengevaluasi tingkat keamanan seed phrase tersebut dan melihat seberapa sulitnya bagi penyerang untuk menebak atau merekonstruksi seed phrase yang tepat.

2. Metode Penelitian

2.1 Gambaran Umum

Pengujian ini akan menggunakan metode serangan brute force. Serangan ini melibatkan pencocokkan suatu pola dengan semua kemungkinan kata antara 0 dan nm untuk menemukan keberadaan suatu pola dalam teks. [1] Dalam konteks ini, pola yang dicocokkan adalah seed phrase yang digunakan dalam sebuah wallet cryptocurrency. Seed phrase yang akan digunakan berjumlah 12 kata yang terdiri dari 2048 kata yang telah ditetapkan dalam standar BIP 39. Proses pencocokkan pola ini akan dilakukan dengan menguji setiap kemungkinan kata dari daftar 2048 kata tersebut untuk melihat apakah pola yang sesuai dengan seed phrase dari dompet kripto dapat ditemukan.

- Pertama, pilih seed phrase yang akan diuji. Dalam kasus ini, seed phrase terdiri dari 12 kata yang harus diputuskan untuk wallet cryptocurrency tertentu, seed phrase yang digunakan adalah 'squirrel adjust thunder journey cheese universe pumpkin fever unique ostrich wine taxi'
- Siapkan daftar kata yang akan digunakan dalam serangan brute force. Dalam konteks ini, daftar kata terdiri dari 2048 kata yang telah ditetapkan dalam standar BIP 39 untuk wallet cryptocurrency.
- Lakukan perulangan kombinasi kata dari daftar kata yang telah disiapkan. Proses ini dilakukan untuk menguji setiap kemungkinan kata dari daftar 2048 kata tersebut.
- Cocokkan kata yang diuji dengan seed phrase dari wallet cryptocurrency. Proses ini bertujuan untuk memastikan apakah kata yang diuji sesuai dengan seed phrase yang digunakan dalam wallet.
- Kata yang cocok dengan seed phrase, maka pola tersebut dianggap ditemukan.

2.2 Serangan Yang digunakan

a. Brute Force

Brute force adalah pendekatan langsung untuk menyelesaikan masalah, biasanya didasarkan pada pernyataan masalah dan definisi konsep yang terlibat. Algoritma brute force bekerja dengan cara yang sangat sederhana, langsung, dan jelas. Dalam pencocokan string, terdapat dua istilah utama: teks dan pola. Teks adalah kata yang dicari dan akan dicocokkan dengan pola. Algoritma Brute Force digunakan untuk memeriksa setiap kemungkinan posisi string dalam teks mulai dari karakter pertama hingga karakter terakhir. Setelah memeriksa karakter pertama, string akan bergeser satu posisi ke kanan, atau karakter akan bergeser ke karakter kedua, ketiga, dan seterusnya. Perbandingan karakter pada teks dapat diselesaikan pada posisi manapun selama proses pencarian, sehingga tidak memerlukan tahap proses tambahan. Sebagai contoh, jika kita memiliki teks "backbone" dan pola yang akan dicocokkan adalah "bone", maka pada karakter pertama "b" akan terjadi kecocokan karena huruf pertama pada pola sama dengan huruf pertama pada teks. Namun, pada karakter kedua "o", terjadi ketidakcocokan karena huruf kedua pada pola tidak sama dengan huruf kedua pada teks. Maka proses pergeseran dilakukan dengan bergeser satu posisi ke kanan. Proses ini akan terus berlanjut sampai seluruh karakter pada pola cocok dengan karakter pada teks. [5]

2.3 Perancangan System

Perancangan sistem dijelaskan dengan flowchart. Secara garis besar system berjalan hanya dengan memanggil kata yang tersedia pada BIP 39 dan kemudian mencocokkan pola kata

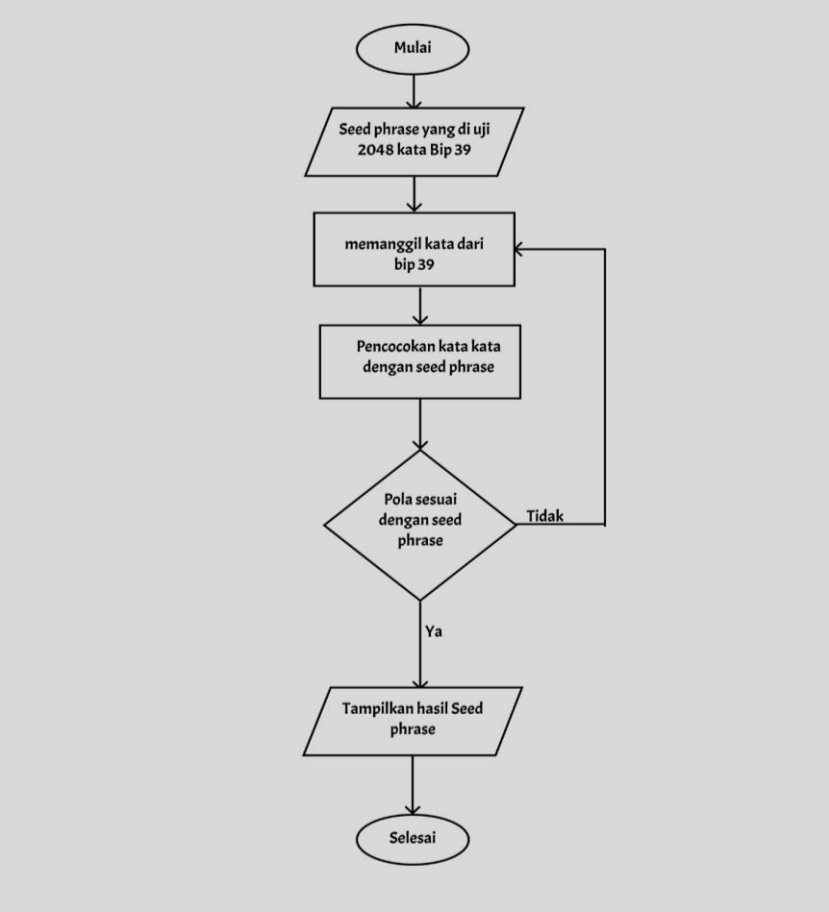
dengan pola kata dari seed phrase yang digunakan yang dijelaskan pada gambar 1.

2.4 Pengujian System

Pengujian system bertujuan untuk mengetahui seberapa jauh tingkat keamanan seed phrase dalam menahan serangan brute force, dan menguji apakah system yang dibuat telah berjalan dengan baik tanpa mengalami error.

3. Hasil dan Pembahasan

3.1 Perancangan Sistem



Gambar 1. Flowchart System

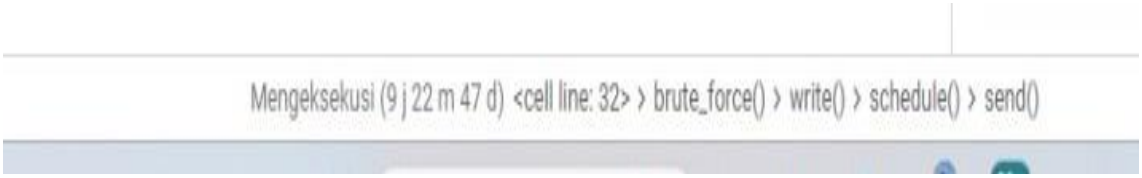
Pada gambar 1 ditunjukan flowchart proses brute force dimulai dengan memanggil pola kata yang ada pada BIP 39, kemudian akan dilakukan proses pencocokan dengan pola kata yang ada pada seed phrase, nantinya jika kata yang dipanggil tidak sesuai dengan seed phrase maka akan diulangi kembali untuk memanggil kata yang ada pada BIP 39, proses ini akan terus berulang hingga pola kata yang dicocokkan sesuai dengan seed phrase, ketika pola berhasil dicocokkan maka system akan berhenti.

p-ISSN: 2986-3929
e-ISSN: 3032-1948

3.2 Pengujian Sistem

```
Streaming output truncated to the last 5000 lines.
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid into
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid invest
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid invite
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid involve
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid iron
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid island
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid isolate
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid issue
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid item
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid ivory
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid jacket
Trying password: abandon ability able about above absent absorb abstract absurd abuse afraid jaguar
```

Gambar 2. Proses pencocokan



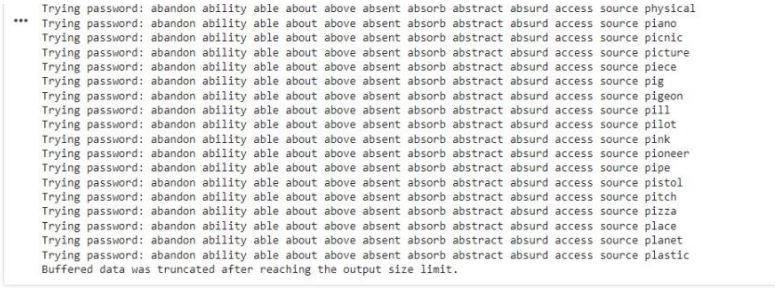
Gambar 3. Waktu Proses pencocokan

Pada gambar 2, kita melihat proses pencocokan kata dari daftar kata BIP 39 dengan pola kata seed phrase yang digunakan. Namun, pada gambar 3, terlihat bahwa meskipun proses tersebut telah berlangsung selama 9 jam, belum ada kata yang cocok ditemukan.

Gambar 4. Error akses memory yang berlebihan

Pada gambar 4 ditunjukan bahwa browser yang digunakan mengalami eror yang dikarenakan jumlah ram memori yang digunakan begitu besar saat menjalankan proses brute force pada seed phrase dengan kombinasi 12 kata

p-ISSN: 2986-3929
e-ISSN: 3032-1948



Gambar 5. Eror dikarenakan ukuran data

Pada gambar 5 diperlihatkan program mengalami eror yang dikarenakan data yang mencapai ukuran batas keluaran.

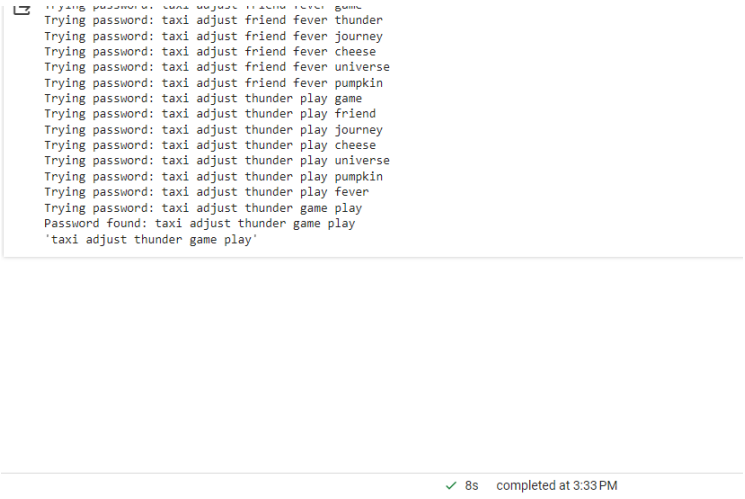
```
# Kata-kata yang akan digunakan
wordlist = ['play', 'game', 'friend', 'adjust', 'thunder', 'journey', 'cheese', 'universe', 'pumpkin', 'fever', 'taxi']


# seedphrase target yang akan dicoba
target_password = 'taxi adjust thunder game play'

# Panjang kata sandi yang akan dicoba
password_length = 5
```

Gambar 6. Pengurangan jumlah kata dari BIP 39

Di gambar 6, dilakukan pengecilan jumlah kata dari daftar BIP yang sebelumnya mencakup 2048 kata menjadi hanya 11 kata yang dipilih. Selain itu, dilakukan juga pemangkasan panjang pola kata yang sedang diuji yang semulanya 12 menjadi 5 kata.



Gambar 7. Output dari password seed phrase dan waktu yang dihabiskan

Gambar 7 menunjukkan hasil akhir dari pencarian seed phrase yang berhasil ditemukan setelah mengurangi jumlah kata yang diambil dari daftar BIP 39 dan memperpendek panjang seed phrase yang diuji. Selain itu, di bagian bawah gambar, disajikan waktu yang diperlukan untuk menemukan pola seed phrase tersebut, yang mencapai 9 detik.

4. Kesimpulan

Dari penelitian yang telah dilakukan, ditemukan bahwa upaya melakukan serangan brute force terhadap seed phrase yang terdiri dari 12 kata, dengan menggunakan 2048 kata yang tersedia dari BIP 39 sangat sulit untuk berhasil dengan kata lain wallet cryptocurrency masih cukup aman. Kompleksitas masalah ini terjadi karena jumlah kombinasi kata yang luar biasa besar, yang dihasilkan dari 2048 pangkat 12 kata yang digunakan. Proses pengujian pada sistem menunjukkan bahwa meskipun telah berjalan selama 9 jam, belum ada hasil yang memuaskan dalam menemukan seed phrase yang sesuai. Kemudian terjadi error ketika memori dan data yang diperlukan untuk proses ini telah mencapai batasnya. Namun, ketika jumlah kata yang digunakan dari BIP 39 dikurangi, proses brute force tersebut dapat diselesaikan dalam waktu yang sangat singkat, kurang dari 10 detik. Penelitian ini menggambarkan bahwa serangan brute force pada wallet cryptocurrency memungkinkan, namun, hal tersebut hanya dapat dicapai dengan menggunakan perangkat yang canggih dan memerlukan waktu yang cukup lama.

Daftar Pustaka

[1] Barutu, C., & Abdi, N. (n.d.). Brute Force Algorithm Implementation of Dictionary Search 1. http://ejournal.seaninstitute.or.id/index.php/InfoSains

[2] Ledger Academy. (n.d.). Understanding BIP-39: The Origin of Your Seed Phrase. Retrieved May 10, 2024, from https://www.ledger.com/academy/bip-39-the-low-key-guardian-of-your-crypto-freedom

[3] Shaik, C. (2020). Securing Cryptocurrency Wallet Seed Phrase Digitally with Blind Key Encryption. International Journal on Cryptography and Information Security, 10(4), 1–10. https://doi.org/10.5121/ijcis.2020.10401

[4] Shaik, C. (2020). Unforgettable User Defined Seed Phrase for Cryptocurrency Wallets. International Journal on Cryptography and Information Security, 10(4), 11–20. https://doi.org/10.5121/ijcis.2020.10402

[5] Sinaga, A. (2021). Aditya Sinaga 1, Nuraisana nuraisana 2 [Sistem Pendukung Keputusan Pemilihan Karyawan Tetap pada Trinity Teknologi Nusantara Dengan Metode Moora. 4(1), 6–15