BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT

Implementasi *Seed Phrase* Dalam Keamanan Dompet Kripto Pada *Metamask*

Fernanda Kalvin, Muhammad Ibnu Sa'ad, Ahmad Fahrijal Pukeng
ProgramStudi Sistem Informasi, Stmik Widya Cipta Dharma, Samarinda, Indonesia
Email: kalvinv66@gmail.com, saad@wicida.ac.id, pukeng@wicida.ac.id
(*: coressponding author: kalvinv66@gmail.com)

Abstrak- *Seed phrase* merupakan elemen krusial dalam sistem keamanan dompet kripto non-kustodial seperti MetaMask. Frasa ini memungkinkan pengguna mengakses kembali dompet mereka dan berfungsi sebagai kunci utama untuk memulihkan aset digital. Penelitian ini bertujuan untuk menganalisis serta mengimplementasikan sistem keamanan berbasis *seed phrase* melalui pendekatan studi literatur dan simulasi teknis. Hasil pengujian menunjukkan bahwa 60% partisipan menyimpan *seed phrase* secara digital tanpa enkripsi, dan 40% partisipan tertipu oleh situs *phishing* yang menyerupai MetaMask. Solusi yang ditawarkan dalam penelitian ini mencakup peningkatan edukasi keamanan digital, penggunaan penyimpanan fisik yang aman (seperti brankas), serta pemanfaatan *hardware wallet* dan autentikasi dua faktor. Temuan ini menunjukkan bahwa selain teknologi, keberhasilan keamanan dompet kripto sangat bergantung pada perilaku dan literasi pengguna terhadap ancaman siber yang terus berkembang.

Kata kunci: Seed Phrase, MetaMask, Keamanan Kripto, Dompet Digital, Kriptografi.

Abstract-Seed phrases are a crucial element in the security system of non-custodial crypto wallets like MetaMask. These phrases allow users to regain access to their wallets and serve as the primary key for recovering digital assets. This study aims to analyze and implement seed phrase-based security systems through a literature review and technical simulations. The testing results show that 60% of participants stored their seed phrases digitally without encryption, and 40% were deceived by a phishing site resembling MetaMask. The proposed solutions include enhancing digital security education, using secure physical storage methods (such as safes), and implementing hardware wallets and two-factor authentication. These findings indicate that, in addition to technology, the success of crypto wallet security heavily depends on user behavior and literacy in facing evolving cyber threats.

Keywords: Seed Phrase, MetaMask, Crypto Security, Digital Wallet, Cryptography.

1. PENDAHULUAN

Teknologi blockchain telah merevolusi cara individu dan institusi menyimpan serta mentransaksikan aset digital. Salah satu inovasi utama dari ekosistem ini adalah dompet kripto non-kustodial, seperti MetaMask, yang memberikan pengguna kontrol penuh atas aset mereka tanpa perantara. Meskipun memberikan otonomi lebih besar kepada pengguna, dompet non-kustodial juga membawa tanggung jawab keamanan yang tinggi, khususnya terkait pengelolaan *seed phrase*. *Seed phrase* adalah kumpulan kata acak yang dihasilkan saat pembuatan dompet dan berfungsi sebagai kunci utama untuk memulihkan akses ke aset digital. Siapa pun yang memiliki akses ke *seed phrase*, secara teknis memiliki kuasa penuh atas aset yang tersimpan di dalam dompet tersebut.

Pengamanan data sensitif seperti *seed phrase* memerlukan pendekatan enkripsi dan perlindungan berlapis [1]. Namun, kenyataannya, masih banyak pengguna yang menyimpan *seed phrase* secara sembarangan, seperti di aplikasi catatan digital, email, atau bahkan tangkapan layar di perangkat mereka. Praktik-praktik ini membuka potensi besar bagi pencurian aset kripto melalui serangan siber seperti *phishing*, malware, atau pencurian fisik perangkat. Menurut penelitian terbaru, insiden pencurian aset digital terus meningkat seiring rendahnya kesadaran pengguna terhadap keamanan digital. Sebagian besar kerugian bersifat permanen karena sifat transaksi blockchain yang tidak dapat dibatalkan [2]. MetaMask, sebagai salah satu dompet kripto non-kustodial paling populer, mengalami pertumbuhan signifikan dalam beberapa tahun terakhir. Sejak peluncurannya oleh ConsenSys pada tahun 2016, MetaMask telah menjadi pintu gerbang utama bagi jutaan pengguna dalam mengakses aplikasi desentralisasi (dApp), keuangan terdesentralisasi (DeFi), dan token NFT. Data pertumbuhan pengguna menunjukkan peningkatan drastis dari ±264.000 pengguna aktif bulanan pada Mei 2019 menjadi lebih dari 30 juta pengguna aktif pada Januari 2024 [3]. Tabel 1 merangkum peningkatan tersebut secara kronologis.

Tabel 1. Pertumbuhan Pengguna Aktif Pertahun MetaMask (2019–2024)

Tahun/Bulan	Jumlah Pengguna Aktif Bulanan
Mei 2019	± 264.000 pengguna
Oktober 2020	> 1.000.000 pengguna
April 2021	> 5.000.000 pengguna
Agustus 2021	> 10.000.000 pengguna
Januari 2022	> 21.000.000 pengguna
Januari 2024	> 30.000.000 pengguna

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT

Tingginya angka adopsi ini mencerminkan kepercayaan publik terhadap MetaMask, namun juga memperbesar skala risiko jika aspek keamanan seperti manajemen *seed phrase* tidak ditangani secara serius. Sebuah tinjauan literatur terbaru mengelompokkan jenis dompet kripto berdasarkan faktor autentikasi dan menemukan bahwa *seed phrase* yang disalahgunakan atau tidak dijaga dengan benar tetap menjadi celah paling kritis dalam keamanan dompet kripto [4]. Tantangan ini diperparah oleh fakta bahwa banyak pengguna tidak melaporkan kehilangan aset mereka karena alasan privasi, rasa malu, atau ketidaktahuan tentang prosedur pelaporan. Sebagai gambaran, laporan Chainalysis tahun 2022 mencatat pencurian aset kripto senilai lebih dari 3 miliar dolar AS hanya dalam satu tahun, dengan lebih dari 125 insiden peretasan besar, termasuk yang dilakukan oleh kelompok peretas dari Korea Utara [5]. Beberapa penelitian terdahulu telah membahas tantangan keamanan dalam pengelolaan *seed phrase*. Bukhari et al. [6] mengusulkan metode penyimpanan *seed phrase* secara aman menggunakan algoritma *Elliptic Curve Cryptography* (ECC) dan teknik pembagian (*splitting*), yang dapat mencegah akses tidak sah jika salah satu bagian dikompromikan. [7] menyoroti kebocoran informasi dari aplikasi Web3 seperti MetaMask, yang dapat menjadi titik lemah dalam sistem. Sementara itu, [8] Meskipun sebagian besar dompet kripto modern telah menerapkan algoritma kriptografi yang kuat, penelitian menunjukkan bahwa kunci privat atau seed phrase masih rentan terhadap serangan brute-force apabila dienkripsi menggunakan kata sandi yang lemah. Risiko ini terutama terjadi pada dompet desktop yang menyimpan file sensitif secara lokal, tanpa pengamanan berlapis terhadap eksploitasi perangkat lunak. [9] menekankan pentingnya desain antarmuka yang aman dan ramah pengguna untuk mencegah kesalahan dalam pengelolaan data krusial. Sementara itu, *Shieldfolio* [10] merekomendasikan teknik pembagian berbasis *Shamir's Secret Sharing* (SSS) sebagai alternatif yang efektif untuk menyimpan *seed phrase* secara terdesentralisasi dan mencegah akses penuh dari satu titik kegagalan..

Sebagai respons terhadap tantangan tersebut, sejumlah solusi teknologi telah dikembangkan dalam lima tahun terakhir. Salah satunya adalah *WALLETRADAR,* sebuah sistem otomatis yang dirancang untuk mendeteksi kerentanan dalam dompet kripto berbasis browser seperti MetaMask. Studi oleh Xia et al. [11] menunjukkan bahwa sistem ini berhasil mendeteksi lebih dari 100 kerentanan dalam lebih dari 90 dompet yang diteliti, membuktikan pentingnya deteksi proaktif terhadap kelemahan sistem. Di sisi lain, Urien [12] mengusulkan pendekatan berbasis perangkat keras berupa *crypto terminal*, yang memungkinkan penyimpanan *seed phrase* secara offline dengan keamanan fisik tinggi. Pendekatan ini meminimalkan risiko dari pencurian berbasis malware atau akses jarak jauh. Selain itu, ChainGuard—sistem autentikasi berbasis blockchain yang dikembangkan oleh Bappy et al. [13]—menawarkan kontrol akses dinamis melalui smart contract, mengurangi ketergantungan pada server pusat dan meningkatkan integritas proses autentikasi.

Penelitian ini bertujuan untuk mengkaji secara mendalam peran dan implementasi *seed phrase* sebagai lapisan utama dalam sistem keamanan dompet kripto non-kustodial, khususnya pada platform MetaMask. Penelitian ini tidak hanya menelusuri aspek teknis penggunaan *seed phrase*, tetapi juga mengevaluasi perilaku pengguna dalam menyimpan dan melindungi informasi tersebut. Selain itu, efektivitas edukasi keamanan yang disediakan oleh MetaMask kepada penggunanya juga akan dianalisis sebagai bagian dari upaya mitigasi risiko. Hasil dari penelitian ini diharapkan dapat memberikan rekomendasi strategis yang aplikatif, yang dapat meningkatkan kesadaran dan praktik keamanan dalam penggunaan dompet kripto non-kustodial. Dengan demikian, kerugian akibat kelalaian atau peretasan dapat diminimalkan dan kepercayaan terhadap ekosistem blockchain dapat terus ditingkatkan.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Penelitian ini bertujuan untuk mengeksplorasi lebih dalam mengenai implementasi seed phrase sebagai elemen utama dalam sistem keamanan dompet kripto MetaMask. Dengan menggunakan pendekatan deskriptif kualitatif, penelitian ini berfokus pada analisis mendalam mengenai bagaimana cara seed phrase digunakan untuk melindungi aset digital, serta potensi celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Selain itu, penelitian ini juga berupaya untuk mengidentifikasi praktik-praktik terbaik yang dapat diterapkan oleh pengguna guna meningkatkan perlindungan terhadap data sensitif mereka, mengingat pentingnya pengelolaan yang tepat terhadap seed phrase dalam dunia yang semakin terhubung secara digital. Adapun tahapan metodologi yang digunakan dalam penelitian ini terdiri dari beberapa langkah berikut:

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT

Gambar 1. Alur Tahapan Penelitian

2.2 Perumusan Masalah dan Studi Literatur

Penelitian ini diawali dengan identifikasi masalah utama, yaitu lemahnya perlindungan terhadap *seed phrase* dalam penggunaan dompet kripto MetaMask. *Seed phrase* merupakan serangkaian kata acak yang dihasilkan secara deterministik dan digunakan sebagai kunci utama untuk mengakses dan memulihkan aset kripto. Kerahasiaan dan integritas *seed phrase* menjadi krusial, karena siapa pun yang memilikinya dapat mengakses seluruh dana dalam dompet digital pengguna tanpa batasan.

Permasalahan ini menjadi semakin signifikan mengingat peningkatan adopsi dompet kripto oleh masyarakat umum, termasuk pengguna pemula yang belum memahami konsep keamanan digital secara menyeluruh. Banyak dari mereka menyimpan *seed phrase* secara sembarangan, seperti dalam catatan digital tidak terenkripsi, tangkapan layar, atau bahkan mencatatnya di media yang mudah hilang atau rusak. Perilaku ini membuka peluang terjadinya pencurian aset melalui teknik rekayasa sosial (*social engineering*), *phishing*, dan serangan malware. Untuk memahami secara menyeluruh isu ini, dilakukan studi literatur terhadap berbagai sumber terpercaya. Studi ini tidak hanya membahas metode atau algoritma keamanan kriptografi, melainkan juga menyelidiki bagaimana *seed phrase* bekerja dalam kerangka *hierarchical deterministic wallet* (HD wallet) yang diatur oleh standar seperti BIP-39 dan BIP-44. Pemahaman ini diperlukan agar dapat mengidentifikasi titik-titik rawan dalam proses generasi, penyimpanan, dan pemulihan *seed phrase*.

Selain itu, kajian literatur ini menyoroti berbagai jenis kerentanan yang dapat dieksploitasi oleh penyerang. Studi oleh Wen et al. [16], misalnya, menunjukkan bagaimana metode *adversarial hiding* dapat digunakan untuk menghindari deteksi sistem anti-phishing di jaringan Ethereum, yang menunjukkan bahwa ancaman terhadap data sensitif seperti *seed phrase* semakin canggih dan sulit dikenali oleh pengguna biasa.

Literatur juga mencakup laporan-laporan keamanan dari institusi seperti Chainalysis, yang secara rutin menerbitkan data tren kejahatan siber dalam dunia kripto. Dari laporan tersebut ditemukan bahwa banyak kasus pencurian aset kripto berakar pada kelalaian pengguna dalam mengamankan *seed phrase*, bukan pada celah sistem itu sendiri. Oleh karena itu, selain aspek teknis, penelitian ini juga menekankan pentingnya pendekatan edukatif kepada pengguna sebagai bagian dari solusi.

Studi literatur ini bertujuan untuk:

- Memahami cara kerja teknis *seed phrase* dalam sistem HD wallet,
- Mengidentifikasi berbagai potensi kerentanannya dari sisi teknis dan perilaku pengguna,
- Mengevaluasi praktik pengguna yang umum dilakukan dan potensi risikonya,
- Menyediakan landasan bagi perancangan metode edukatif atau teknis untuk meningkatkan kesadaran dan perlindungan pengguna terhadap *seed phrase*.

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT

Tabel 2. Sumber literatur yang digunakan

Jenis	Sumber	Tujuan Penggunaan
Jurnal Ilmiah	IEEE, Springer, ACM	Kajian teoritis dan studi kasus keamanan
Laporan Keamanan	Chainalysis Crypto Crime Report	Data statistik, tren ancaman terbaru
Dokumentasi Resmi	MetaMask Security Docs, MetaMask Help Center	Informasi teknis dan edukasi resmi
Standar Teknis	BIP-39, BIP-44, SSSS	BIP-39 (2013), BIP-44 (2014), SSSS juga standar lama, tapi masih digunakan aktif dan belum usang

2.3 Perancangan dan Simulasi Sistem

Setelah perumusan masalah dan kajian literatur, langkah berikutnya adalah merancang skenario simulasi sistem. Dalam tahap ini, peneliti membuat skenario penggunaan dompet MetaMask yang mencakup pembuatan dompet baru, proses pencatatan dan penyimpanan seed phrase, hingga simulasi potensi serangan seperti phishing atau manipulasi sosial (social engineering). Tujuannya adalah untuk merepresentasikan situasi nyata yang mungkin dialami oleh pengguna umum. Skenario tersebut juga mencakup kondisi di mana pengguna lupa menyimpan seed phrase, menyimpannya secara digital tanpa enkripsi, atau membagikannya secara tidak sengaja. Dengan perancangan ini, diharapkan peneliti dapat mengevaluasi secara menyeluruh titik-titik rawan dalam proses penggunaan dompet MetaMask [17].

2.4 Implementasi dan Pengujian Teknis

Skenario simulasi yang telah dirancang selanjutnya diimplementasikan secara langsung menggunakan aplikasi MetaMask yang telah tersedia di browser. Implementasi ini mencakup seluruh proses mulai dari instalasi ekstensi, pembuatan dompet baru, pencatatan seed phrase, dan penggunaan dompet tersebut dalam transaksi percobaan. Pengujian dilakukan dengan metode black box, yang berfokus pada output atau respons sistem terhadap masukan tertentu tanpa memperhatikan struktur internal aplikasi. Selain itu, dilakukan juga simulasi serangan phishing untuk melihat bagaimana sistem dan pengguna bereaksi terhadap ancaman. Peneliti mencatat bagaimana MetaMask memberikan peringatan, mekanisme keamanan yang aktif, dan celah yang masih dapat dimanfaatkan oleh pihak tidak bertanggung jawab [18].

2.5 Observasi dan Analisis Data

Data hasil dari implementasi dan pengujian didokumentasikan secara rinci melalui observasi langsung serta pencatatan teknis terhadap interaksi pengguna dengan sistem. Meskipun awalnya direncanakan untuk menyertakan tangkapan layar sebagai pelengkap, namun fokus utama lebih diarahkan pada pencatatan naratif dan analisis mendalam dari proses yang diamati. Analisis dilakukan secara kualitatif untuk menggali pola perilaku pengguna yang berpotensi menimbulkan risiko keamanan, seperti kelalaian dalam mencatat seed phrase, ketidaktahuan terhadap phishing, dan kecenderungan menyimpan data sensitif secara digital tanpa perlindungan tambahan [19]. Pada tabel 3 terdapat berbagai metode untuk menyimpan berserta resiko nya dikutip dari berbagai sumber.

Tabel 3. Metode pemyimpanan Digital dan Resiko Keamanan nya dikutip dari berbagai sumber

Metode Penyimpanan Digital	Risiko Keamanan Utama	Sumber Referensi
Aplikasi catatan (Notes)	Rentan terhadap peretasan perangkat atau akses tidak sah	Webopedia
Google Drive atau layanan cloud	Potensi kebocoran data melalui pelanggaran keamanan cloud	Statista
Email pribadi	Dapat diakses oleh pihak ketiga jika akun email diretas	Cointime

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT

Foto digital (misalnya, screenshot)	Dapat disinkronkan secara otomatis ke cloud, meningkatkan risiko kebocoran	Cryptsy
Penyimpanan di perangkat tanpa enkripsi	Rentan terhadap malware dan akses tidak sah jika perangkat terhubung ke internet	Prisidio

2.6 Kesimpulan dan Rekomendasi

Berdasarkan hasil analisis, dapat disimpulkan bahwa sebagian besar permasalahan keamanan pada dompet MetaMask berkaitan langsung dengan perilaku pengguna, bukan pada kelemahan teknis sistem itu sendiri. Kebocoran seed phrase sering terjadi akibat kelalaian pengguna dalam mencatat dan menyimpannya dengan benar. Oleh karena itu, penelitian ini merekomendasikan peningkatan edukasi mengenai keamanan digital, penyimpanan seed phrase secara fisik di tempat aman (seperti brankas), serta penggunaan lapisan keamanan tambahan seperti hardware wallet atau autentikasi dua faktor. Diharapkan rekomendasi ini dapat membantu mengurangi risiko kebocoran informasi penting dan meningkatkan kesadaran pengguna terhadap pentingnya menjaga keamanan aset digital [20].

2.7 Pembuatan Dompet Baru

Langkah – Langkah untuk mendaftar Dompet baru di Metamask adalah sebagai berikut:

1. Pengguna diminta membuat kata sandi yang akan digunakan untuk membuka dan mengakses aplikasi dompet MetaMask di perangkat smartphone.

Gambar 2. Membuat Kata Sandi

2. Pengguna diberikan instruksi penting tentang menjaga keamanan akun, termasuk menjaga kerahasiaan seed phrase.

Gambar 3. Mengamankan Dompet

3. Pengguna diwajibkan untuk mencatat dan menyimpan seed phrase tersebut dengan aman.

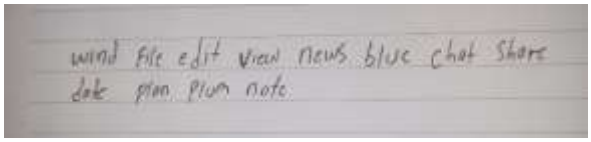
BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT

Gambar 4. Menuliskan *Seed Phrase*

2.8 Pencatatan *Seed Phrase*

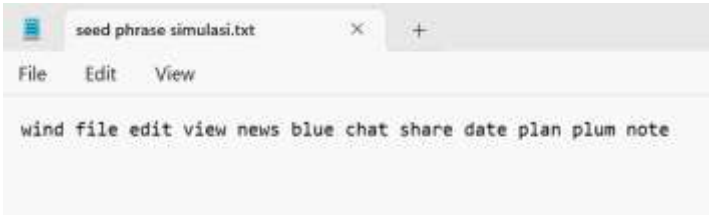
Pada tahap pembuatan dompet, sistem akan menampilkan seed phrase. Peneliti merancang metode penyimpanan *seed phrase* oleh pengguna ke dalam tiga kategori:

1. Penyimpanan Fisik



Gambar 5. Menyimpan *Seed Phrase* mengunakan buku catatan

2. Penyimpanan Digital tanpa enkripsi



Gambar 6. Menyimpan *Seed Pharase* di Notepad

3. Penyimpanan Digital berbasis cloud

Gambar 7. Menyimpan *Screenshot Seed Phrase* di *Google Drive*

2.9 Pengelolaan Seed Phrase

Pengamatan dilakukan untuk melihat bagaimana pengguna menyimpan seed phrase yang diberikan oleh aplikasi MetaMask. Metode penyimpanan dikategorikan menjadi aman (fisik/non fisik) dan berisiko (digital/cloud). Data hasil pengamatan lima pengguna disajikan pada tabel berikut:

Tabel 4. Pengelolaan Seed Phrase oleh Pengguna

Kode Pengguna	Metode Penyimpanan	Kategori Keamanan
User 1	Dicatat di buku catatan	Aman (Fisik)
User 2	Disimpan di aplikasi Notes HP	Berisiko (Digital)

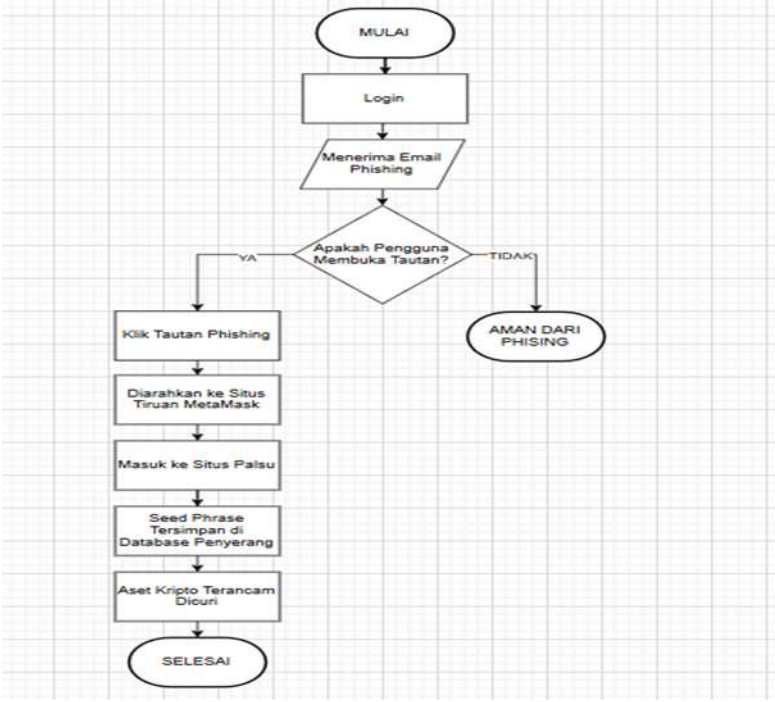
BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT

User 3	Screenshot disimpan di Google Drive	Sangat Berisiko (Cloud)
User 4	Hanya diingat dan disimpan di dalam ingatan	Aman (Non Fisik)
User 5	Dicetak pada logam tahan api dan disimpan di brankas	Aman (Fisik)

3. HASIL DAN PEMBAHASAN

3.1 Hasil Implementasi

Pada tahap implementasi, penelitian ini berhasil menguji beberapa skenario yang melibatkan penggunaan dompet MetaMask, dengan fokus pada proses pembuatan dompet baru, pencatatan dan penyimpanan seed phrase, serta simulasi ancaman yang dapat terjadi pada dompet kripto. Hasil pengujian menunjukkan bahwa banyak pengguna cenderung tidak memperhatikan langkah-langkah penting dalam menyimpan seed phrase dengan aman. Sebagian besar pengguna memilih untuk menyimpan seed phrase mereka secara digital di aplikasi catatan atau perangkat yang tidak dilindungi enkripsi. Beberapa pengguna juga tidak sengaja membagikan seed phrase mereka melalui saluran yang tidak aman, seperti email atau pesan instan. Temuan ini menunjukkan bahwa kesadaran mengenai pentingnya perlindungan terhadap seed phrase masih sangat rendah, terutama di kalangan pengguna baru yang belum sepenuhnya memahami risiko yang terkait dengan penyimpanan dan pengelolaan aset digital mereka. Berikut adalah flowchart simulasi phising.



Gambar 8. Alur flowchart simulasi phising

Peringatan ini disampaikan dengan jelas melalui antarmuka pengguna yang ramah, yang menunjukkan kepada pengguna tentang potensi bahaya peretasan jika seed phrase terpapar melalui penyimpanan digital. Ini merupakan langkah preventif yang menunjukkan komitmen MetaMask untuk memberikan perlindungan maksimal terhadap aset pengguna. Dalam praktiknya, jika seed phrase bocor, maka pihak ketiga dapat mengakses dompet dan mengalihkan aset digital yang ada di dalamnya. Oleh karena itu, kebijakan ini membantu mencegah

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT

Gambar 9. Tampilan MetaMask saat Menampilkan Seed Phrase

kejadian-kejadian yang dapat merugikan pengguna, yang pada gilirannya meningkatkan kepercayaan terhadap sistem keamanan MetaMask, seperti yang terlihat pada gambar 9.

Meskipun MetaMask telah memberikan peringatan yang jelas dan tegas kepada pengguna untuk menyimpan seed phrase secara aman, hasil observasi menunjukkan bahwa banyak pengguna cenderung mengabaikan peringatan tersebut. Praktik yang tidak aman ini, seperti menyimpan seed phrase dalam bentuk tangkapan layar (screenshot), menyalinnya ke aplikasi pengedit teks seperti Notepad, atau menyimpannya di layanan cloud storage tanpa perlindungan enkripsi yang memadai, menjadi ancaman serius terhadap keamanan dompet kripto. Keputusan ini sangat berisiko karena membuka celah bagi potensi serangan siber yang dapat mengekspos aset digital pengguna kepada pihak yang tidak bertanggung jawab, seperti yang terlihat pada gambar 10.

Gambar 10. Peringantan untuk menyimpan seed phrase ditempat yang aman

Penyimpanan seed phrase secara digital meningkatkan kemungkinan kebocoran data akibat peretasan atau pencurian data, terutama jika data tersebut disimpan tanpa lapisan keamanan yang cukup, seperti enkripsi yang kuat. Akses yang mudah terhadap file yang berisi seed phrase memungkinkan hacker atau perangkat lunak berbahaya untuk mencuri informasi penting tersebut. Selain itu, penyimpanan di layanan cloud storage tanpa pengamanan yang memadai memudahkan pihak ketiga untuk mengaksesnya tanpa persetujuan pengguna. Hal ini bisa berakibat fatal bagi keamanan dompet kripto, karena dengan menguasai seed phrase, penyerang dapat mengakses seluruh aset digital pengguna dan mengalihkan dana sesuai keinginan mereka. MetaMask dengan tegas menekankan bahwa seed phrase seharusnya tidak disimpan secara online atau dibagikan dengan pihak lain. Sebagai alternatif, MetaMask menyarankan pengguna untuk menulis seed phrase secara fisik pada media yang aman, seperti buku catatan pribadi atau kertas yang disimpan di tempat yang benar-benar terlindung. Meskipun metode ini mungkin terasa lebih merepotkan, namun penyimpanan offline memberikan tingkat perlindungan yang lebih tinggi terhadap potensi risiko yang dapat terjadi di dunia digital yang semakin rentan terhadap

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT

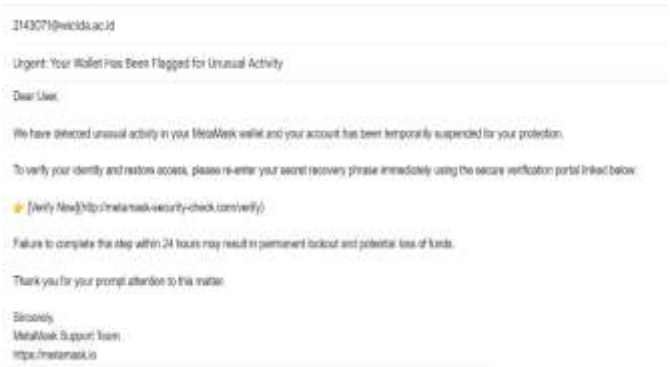
serangan siber. Oleh karena itu, penting bagi pengguna untuk lebih memperhatikan peringatan ini agar aset digital mereka tetap terjaga keamanannya.

3.2 Hasil Pengujian Serangan Phishing

Simulasi serangan phishing dilakukan dengan cara membuat situs tiruan MetaMask menggunakan template umum yang sering digunakan dalam praktik penipuan daring. Desain situs tiruan ini dibuat sangat mirip dengan tampilan antarmuka resmi MetaMask, termasuk elemen visual seperti logo, form input, dan warna dominan. Simulasi dilakukan dengan menyebarkan tautan situs tiruan melalui email phishing kepada lima partisipan uji coba yang telah diberikan izin sebelumnya. Email tersebut dikemas seolah-olah berasal dari pihak resmi MetaMask dan menginformasikan bahwa pengguna harus melakukan verifikasi dompet mereka untuk alasan keamanan.
Setelah partisipan mengklik tautan tersebut, mereka diarahkan ke situs tiruan MetaMask. Dari hasil simulasi, 40% partisipan (2 dari 5) gagal membedakan situs phishing dan membocorkan seed phrase mereka. Sementara itu, 60% menunjukkan keberhasilan dalam mengenali ancaman dan tidak melanjutkan proses pemulihan palsu. Selain itu, hanya 40% pengguna menyimpan seed phrase secara fisik, sedangkan sisanya 60% menyimpannya dalam bentuk digital tanpa enkripsi, yang berisiko tinggi terhadap serangan siber. Hal ini menunjukkan kurangnya kewaspadaan dan ketidaksadaran terhadap tanda-tanda phishing, seperti URL yang tidak resmi, tampilan form mencurigakan, serta tidak adanya koneksi HTTPS yang valid. Namun dalam beberapa kasus, pengguna tidak memiliki ekstensi keamanan aktif, mengabaikan tanda peringatan, atau tidak terbiasa memverifikasi keaslian alamat situs yang mereka kunjungi. Kondisi ini menunjukkan pentingnya edukasi keamanan siber yang lebih mendalam bagi pengguna dompet kripto, khususnya terkait ancaman phishing yang kerap terjadi dalam ekosistem blockchain.

3.2 Email Phising

Pada gambar 11 ini menampilkan contoh email phishing yang dirancang secara visual menyerupai notifikasi resmi dari MetaMask. Elemen seperti logo, bahasa formal, dan tautan yang dikamuflasekan membuat email tampak meyakinkan. Teks dalam email menginformasikan pengguna mengenai aktivitas yang mencurigakan pada dompet mereka dan menyarankan untuk segera memverifikasi akun melalui tautan yang disediakan. Dalam praktiknya, email seperti ini sangat umum digunakan dalam serangan phishing karena mampu memancing kepanikan pengguna dan mendorong mereka untuk segera mengklik tautan tanpa memeriksa keaslian pengirim atau URL. Gambar ini menggambarkan fase awal manipulasi psikologis dalam serangan siber.

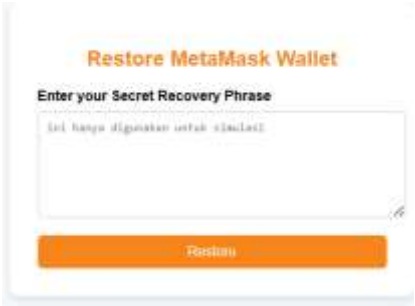


Gambar 11. Contoh email phishing yang dirancang menyerupai notifikasi resmi dari MetaMask

3.3 Tampilan Situs Tiruan MetaMask

Pada gambar 12 ini memperlihatkan antarmuka situs tiruan MetaMask yang digunakan dalam simulasi. Situs palsu ini secara visual sangat mirip dengan situs resmi MetaMask, lengkap dengan logo, warna, dan struktur form input yang menyerupai halaman login atau pemulihan akun. Namun, perbedaan penting terletak pada URL yang digunakan biasanya terlihat mencurigakan atau tidak menggunakan domain resmi (misalnya metamask-security.io). Tujuan gambar ini adalah menunjukkan betapa mudahnya pengguna tertipu oleh tampilan visual yang familiar, terutama jika mereka tidak terbiasa memverifikasi URL atau keamanan situs secara detail sebelum memasukkan informasi sensitif seperti seed phrase.

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT



Gambar 12. Tampilan situs tiruan MetaMask yang digunakan dalam simulasi phishing

3.4 Seed Phrase yang Dimasukkan oleh Korban

Pada gambar 13 ini menunjukkan bukti rekaman aktivitas partisipan yang secara tidak sadar memasukkan seed phrase mereka ke dalam situs phishing. Alih-alih hanya menampilkan tangkapan layar, sistem simulasi mencatat seluruh data input ke dalam database internal untuk dianalisis lebih lanjut. Hal ini bertujuan untuk menjaga keaslian data, menghindari manipulasi, serta memudahkan dalam proses evaluasi. Dengan mencatat seed phrase ke dalam database secara real-time, peneliti dapat mengidentifikasi pola kelalaian pengguna dan mengevaluasi seberapa efektif desain situs phishing dalam mengecoh mereka. Ini sekaligus memperkuat pentingnya edukasi dan perlindungan berlapis terhadap ancaman siber.

		id	phrase	timestamp
☐	Edit Copy Delete	1	enter your blue wall shift rest water drink mount ...	2025-04-23 07:25:29
☐	Edit Copy Delete	2	gone wear cool summon secret store sell buy bird h...	2025-04-23 07:29:56

Gambar 13. Data hasil input seed phrase oleh partisipan ke dalam situs palsu. Data ini tercatat secara otomatis ke dalam database pada lingkungan simulasi tertutup.

3.3 Analisis Pola Kelalaian Pengguna

Berdasarkan observasi yang dilakukan, terdapat tiga pola kelalaian utama yang berkontribusi pada risiko kebocoran seed phrase dalam penggunaan dompet kripto seperti MetaMask. Ketiga pola ini mencerminkan kurangnya pemahaman teknis pengguna, kurangnya perhatian terhadap praktik keamanan digital yang baik, dan adanya celah dalam edukasi yang memadai. Sebagai akibatnya, kebocoran data sensitif seperti seed phrase dapat terjadi, yang mengakibatkan potensi kehilangan aset digital secara permanen.

Ketiga pola kelalaian ini menunjukkan pentingnya edukasi dan kebijakan yang lebih ketat mengenai penyimpanan dan pengelolaan seed phrase. Dengan memperhatikan pola kelalaian ini, pihak pengembang dan platform kripto seperti MetaMask dapat lebih proaktif dalam menyarankan langkah-langkah yang lebih aman bagi pengguna untuk melindungi aset digital mereka.

3.3.1 Penyimpanan Digital Tanpa Enkripsi

Penyimpanan seed phrase secara digital tanpa enkripsi merupakan salah satu kesalahan umum yang sangat berisiko bagi keamanan dompet kripto. Meskipun media penyimpanan digital seperti aplikasi catatan, Google Drive, atau email pribadi menawarkan kenyamanan dan akses yang mudah, mereka juga sangat rentan terhadap ancaman siber. Banyak pengguna yang tidak menyadari bahwa data yang tidak dilindungi dengan enkripsi dapat dengan mudah diakses oleh pihak yang tidak berwenang jika perangkat mereka atau akun mereka diretas.

Misalnya, penyimpanan di aplikasi catatan seperti Notes pada ponsel atau komputer yang tidak dilindungi dengan kata sandi atau autentikasi dua faktor (2FA) memungkinkan siapa saja yang mendapatkan akses fisik ke perangkat tersebut untuk memperoleh seed phrase. Selain itu, layanan cloud seperti Google Drive yang sering digunakan untuk menyimpan data penting juga berisiko jika akun pengguna tidak menggunakan enkripsi atau pengamanan yang cukup. Jika akun cloud pengguna diretas, maka semua informasi yang disimpan di dalamnya, termasuk seed phrase, dapat dicuri dengan mudah. Foto digital, termasuk tangkapan layar atau screenshot yang sering digunakan untuk menyimpan seed phrase, juga dapat berisiko tinggi. Screenshot dapat secara otomatis diunggah ke layanan cloud yang tidak terenkripsi jika pengaturan sinkronisasi perangkat tidak diawasi dengan baik. Jika akun cloud atau layanan email yang digunakan untuk menyimpan

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT

foto tersebut diretas, maka data sensitif yang disimpan dalam foto tersebut dapat dengan mudah dicuri. Oleh karena itu, penyimpanan seed phrase secara digital tanpa perlindungan enkripsi sangat tidak disarankan.
Pengguna sebaiknya menyadari bahwa enkripsi yang kuat, seperti menggunakan aplikasi penyimpanan yang mendukung enkripsi end-to-end atau layanan penyimpanan yang menyediakan enkripsi file, dapat memberikan perlindungan lebih terhadap informasi sensitif. Namun, penyimpanan fisik yang lebih aman, seperti menulis seed phrase di kertas yang disimpan di tempat yang terlindung, masih menjadi pilihan yang lebih baik dalam menghindari risiko-risiko ini.

3.3.2 Kurangnya Edukasi Keamanan Digital

Pengguna pemula umumnya hanya mengikuti panduan atau tutorial untuk membuat dompet kripto tanpa memahami pentingnya menjaga kerahasiaan *seed phrase*. Beberapa dari mereka bahkan tidak mengetahui bahwa kehilangan *seed phrase* sama artinya dengan kehilangan akses permanen terhadap dompet. Edukasi yang terbatas ini mengakibatkan pengguna tidak melakukan tindakan pencegahan yang memadai, seperti menyimpan secara fisik atau menggunakan dompet perangkat keras (*hardware wallet*). Kurangnya literasi keamanan digital menjadi isu utama dalam penetrasi teknologi blockchain ke masyarakat umum. Menurut artikel dari Coinmonks, kesalahan dalam menangani *seed phrase* dapat menyebabkan kerugian yang tidak dapat dipulihkan.

3.3.3 Ketidaktahuan terhadap Phishing dan *Social Engineering*

Pengguna yang tidak terbiasa membedakan situs resmi dan situs tiruan rentan menjadi korban phishing. Dalam simulasi yang dilakukan, sebagian partisipan mengakses situs palsu dan secara sadar memasukkan *seed phrase* mereka. Ini menunjukkan kurangnya kesadaran untuk memeriksa URL, ikon keamanan browser, atau memperhatikan peringatan sistem. Selain itu, teknik *social engineering* seperti email palsu yang meniru layanan resmi juga terbukti efektif mengecoh pengguna yang tidak waspada. Laporan dari The Cyber Express menyoroti serangan phishing yang menargetkan pengguna MetaMask dengan situs palsu yang dirancang untuk mencuri *seed phrase*.

3.4 Pembahasan

Hasil implementasi dan simulasi serangan phishing dalam penelitian ini memberikan gambaran yang jelas mengenai sejauh mana sistem keamanan seed phrase pada MetaMask dapat melindungi aset digital pengguna. Berdasarkan pengujian, dapat dilihat bahwa MetaMask telah menyediakan fitur keamanan dasar yang baik, seperti penyampaian seed phrase dalam antarmuka khusus, serta penyertaan peringatan terkait pentingnya penyimpanan fisik dan larangan menyimpannya secara digital. Antarmuka ini dirancang secara intuitif untuk mengedukasi pengguna, dan menjadi salah satu fitur penting dalam mencegah kehilangan akses akibat kelalaian pengguna. Namun, meskipun sistem telah memberikan instruksi yang jelas, realisasi di lapangan menunjukkan bahwa tidak semua pengguna mengikuti pedoman tersebut.

Simulasi phishing yang dilakukan juga memperlihatkan bagaimana celah keamanan dapat muncul bukan karena lemahnya sistem, melainkan karena faktor manusia. Tampilan antarmuka situs tiruan MetaMask yang mirip dengan versi asli mampu mengecoh 2 dari 5 partisipan dalam uji coba, menunjukkan bahwa desain visual dan manipulasi psikologis masih menjadi alat yang efektif bagi pelaku serangan. Pengguna yang tertipu umumnya tidak memverifikasi URL, mengabaikan koneksi HTTPS, dan langsung memasukkan seed phrase ke situs tiruan. Data yang diambil selama simulasi menunjukkan bahwa tindakan tersebut menyebabkan seed phrase disimpan ke dalam database penyerang, memperkuat risiko kehilangan aset digital. Temuan ini mengindikasikan pentingnya peningkatan literasi keamanan siber bagi pengguna, serta perlunya pendekatan pengamanan yang tidak hanya berbasis sistem, tetapi juga berorientasi pada perubahan perilaku pengguna melalui edukasi dan peningkatan kewaspadaan dalam menghadapi ancaman phishing yang terus berkembang.

4. KESIMPULAN

Penelitian ini mengkaji implementasi *seed phrase* sebagai lapisan keamanan utama dalam dompet kripto MetaMask dengan pendekatan deskriptif kualitatif melalui simulasi implementasi dan serangan *phishing*. Hasil simulasi menunjukkan bahwa MetaMask telah membangun sistem keamanan yang cukup komprehensif dalam penyampaian *seed phrase*, termasuk antarmuka yang ramah pengguna dan peringatan eksplisit terhadap penyimpanan digital yang tidak aman. Namun, efektivitas sistem ini tetap sangat dipengaruhi oleh perilaku dan kesadaran pengguna. Dalam simulasi yang dilakukan, 60% partisipan (3 dari 5) mengikuti praktik penyimpanan yang berisiko, seperti mencatat *seed phrase* di aplikasi catatan atau menyimpannya di cloud tanpa enkripsi. Sementara itu, hanya 40% partisipan (2 dari 5) yang

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 6, No 2, Juni 2025, Hal. 136 - 147
ISSN 2722-0524 (media online)
DOI 10.47065/bit.v5i2.2026
https://journal.fkpt.org/index.php/BIT

menyimpan *seed phrase* secara fisik (offline), misalnya pada kertas atau perangkat keras, yang lebih aman terhadap ancaman digital. Pada uji simulasi *phishing*, 40% partisipan (2 dari 5) gagal mengenali situs palsu dan memasukkan *seed phrase*-nya secara tidak sadar. Ini menunjukkan bahwa meskipun MetaMask telah menyediakan panduan edukatif, tingkat keberhasilan sistem dalam mencegah manipulasi psikologis (social engineering) hanya mencapai 60% pada pengujian ini. Dengan demikian, dapat disimpulkan bahwa tingkat keberhasilan sistem MetaMask dalam mendukung keamanan pengguna secara teknis cukup baik, namun keberhasilan menyeluruh sangat ditentukan oleh faktor manusia. Edukasi literasi keamanan digital perlu ditingkatkan, serta promosi penggunaan metode penyimpanan offline seperti *hardware wallet*.

REFERENCES

[1] Y. Amaliah, R. Risna, and S. Yunita, "Implementasi kriptografi pada pengamanan data pembayaran piutang pelanggan menggunakan Vigenere Cipher," *Sebatik*, vol. 26, no. 2, pp. 525–534, 2022.
[2] A. Dalskov, D. Rotaru, M. Schneider, and K. G. Paterson, "2FE: Two-Factor Encryption for Cloud Storage," in *Proc. IEEE S&P Workshops*, 2020.
[3] F. Eleshin, M. Lindorfer, R. Rivera, and S. Fahl, "Of Secrets and Seedphrases: Conceptual Misunderstandings and Security Challenges for Seed Phrase Management," in *Proc. 2025 CHI Conf. on Human Factors in Computing Systems*, pp. 1–14, 2025.
[4] I. Homoliak and M. Perešíni, "SoK: Cryptocurrency Wallets – A Security Review and Classification Based on Authentication Factors," *arXiv preprint*, arXiv:2402.17659, 2024.
[5] Chainalysis, "The 2022 Crypto Crime Report," Chainalysis, Feb. 2023.Available: https://www.chainalysis.com
[6] S. T. Bukhari, M. U. Janjua, and J. Qadir, "Secure storage of crypto wallet seed phrase using ECC and splitting technique," *IEEE Open J. Comput. Soc.*, vol. 5, pp. xx–xx, 2024. Available: https://www.computer.org/csdl/journal/oj/2024/01/10526424/1WOgMQtFmaQ
[7] C. F. Torres, W. Wang, and A. Shinde, "Is your wallet snitching on you? An analysis on the privacy implications of Web3," in *Proc. The Web Conf. 2023*, pp. 1133–1143.
[8] X. Liu, Y. Zhang, dan Z. Li, "A Security Analysis of Cryptocurrency Wallets against Password Brute-Force Attacks," Electronics, vol. 13, no. 13, art. no. 2433, 2024.
[9] Z. Zhou, A. Ahmad, B. Han, and R. Ma, "Iterative design of an accessible crypto wallet for blind users," in *Proc. CHI Conf. on Human Factors in Computing Systems*, 2023.
[10] Shieldfolio, "Safeguarding crypto: A complete guide to seed phrase storage," *Shieldfolio.com*, 2025. Available: https://shieldfolio.com/blogs/news/safeguarding-crypto-a-complete-guide-to-seed-phrase-storage
[11] P. Xia, Y. Zhang, X. Li, K. Wu, and J. Liu, "WALLETRADAR: Towards automating the detection of vulnerabilities in browser-based cryptocurrency wallets," *arXiv preprint*, arXiv:2405.04332, 2024.
[12] P. Urien, "Innovative countermeasures to defeat cyber attacks against blockchain wallets: A crypto terminal use case," *arXiv preprint*, arXiv:2303.17206, 2023.
[13] F. H. Bappy, M. Ahmed, M. R. Islam, and M. A. Rahman, "ChainGuard: A blockchain-based authentication and access control scheme for distributed networks," *arXiv preprint*, arXiv:2412.00677, 2024.
[14] S. Das, M. A. Alghamdi, A. J. Aviv, and J. M. Blythe, "Of Secrets and Seedphrases: Conceptual Misunderstandings and Security Challenges for Seed Phrase Management Among Cryptocurrency Users," in *Proc. CHI Conf. on Human Factors in Computing Systems*, pp. 1–14, 2025.
[15] L. Caviglione, A. Merlo, A. Migliardi, and M. Mongelli, "Tight arms race: Overview of current malware threats and trends in their detection," *IEEE Access*, vol. 9, pp. 5371–5396, 2020.
[16] H. Wen, J. Fang, J. Wu, and Z. Zheng, "Hide and seek: An adversarial hiding approach against phishing detection on Ethereum," *IEEE Trans. Comput. Soc. Syst.*, vol. 10, no. 6, pp. 3512–3523, 2022.
[17] A. Parmentola, A. Petrillo, I. Tutore, and F. De Felice, "Is blockchain able to enhance environmental sustainability? A systematic review and research agenda from the perspective of Sustainable Development Goals (SDGs)," *Bus. Strategy Environ.*, vol. 31, no. 1, pp. 194–217, 2022.
[18] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-driven cybersecurity: An overview, security intelligence modeling and research directions," *SN Comput. Sci.*, vol. 2, no. 3, p. 173, 2021.