International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Crypto Currency Wallet Security Checker

Jambu Vishnu Vardhan Reddy[1], M.Purna Chandu[2], K.Naresh[3], Dr.S.Mohandoss[4]

1,2,3Student of CFIS, Dr.M.G.R Educational And Research Institute Chennai, India
[4]Associate Professor of CFIS, Dept of CSE, Dr.M.G.R Educational And Research Institute Chennai, India
[1]jvishnuvardhanreddy.cfis@gmail.com, [2]maneepallipurnachandu@gmail.com, [3]knaresh@gmail.com, [4]Mohandoss.cse@drmgrdu.ac.in

Abstract: With the rising adoption of digital currencies, securing cryptocurrency wallets is a crucial concern. This paper presents the development of a Cryptocurrency Wallet Security Checker, a comprehensive tool designed to assess and enhance wallet security by evaluating authentication mechanisms, seed phrase management, phishing risks, and other security parameters. The system provides real-time security recommendations and generates detailed reports to improve user awareness and protection. Experimental results demonstrate the tool's effectiveness in detecting vulnerabilities and providing actionable insights for users.

Keywords: Cryptocurrency Wallet, Security Assessment, Phishing Detection, Two-Factor Authentication, Password Strength, Cybersecurity.

1. Introduction

Cryptocurrency wallets are essential for securely storing and managing digital assets. However, due to the decentralized nature of blockchain transactions, they are highly targeted by cybercriminals. Attacks on wallets,

including phishing, malware, and brute-force attacks, have led to significant financial losses. This paper introduces a Cryptocurrency Wallet Security Checker to assess wallet security, identify vulnerabilities, and provide recommendations for improvement.

2. Literature Review

Existing research highlights various vulnerabilities in cryptocurrency wallets, including weak passwords, inadequate two-factor authentication (2FA), and poor seed phrase storage practices. Studies have explored phishing detection techniques, secure authentication methods, and real-time threat monitoring. The proposed tool integrates insights from these studies to create a robust security assessment system.

3. Methodology

3.1 System Architecture

the Cryptocurrency Wallet Security Checker follows a client-server model with local security checks for privacy protection. The architecture includes a frontend interface for user interaction, a backend for security assessment, and APIs for phishing detection.

Diagram 1: System Architecture

[User] --> [Frontend UI] --> [Backend Server] --> [Phishing Detection API]

3.2 Security Assessment Modules

Module	Function
Password Strength Analysis	Evaluates password complexity and suggests improvements.
Two-Factor Authentication (2FA) Verification	Checks for 2FA implementation and provides recommendations.
Seed Phrase Protection	Advises users on secure storage practices.
Phishing Detection	Scans wallet URLs against a phishing database.
Security Report Generation	Compiles security findings into a downloadable report.

3.3 Implementation The system is built using JavaScript (React.js) for the frontend, Node.js for the backend, and integrates APIs such as Google Safe Browsing for phishing detection. Password strength evaluation uses entropy-based analysis.

4. Experimental Results and Performance Analysis

4.1 Response Time Security assessments are completed within 3–5 seconds, ensuring a seamless user experience.

Security Check	Average Response Time
Password Strength Analysis	1-2 seconds
2FA Verification	1-2 seconds
Seed Phrase Security Evaluation	2-3 seconds
Phishing Detection via API	3-5 seconds
Report Generation	2 seconds

4.2 Accuracy of Security Checks

Security Feature	Accuracy (%)	False Positives (%)
Password Strength Checker	98%	2%
2FA Verification	99%	1%
Seed Phrase Security	97%	3%
Phishing Detection	96%	4%

4.3 Scalability and Load Testing The system maintains stable performance up to 500 concurrent users, with minor delays at higher loads.

Number of Users	Average Response Time	System Status
50	2.5s	Stable
100	3.0s	Stable
250	4.2s	Stable
500	5.8s	Slightly Delayed
1000	8.0s	Degraded Performance

4.4 User Experience Evaluation Usability tests show a 92% satisfaction rate, with users finding the tool intuitive and effective.

Factor	User Satisfaction (%)
Ease of Use	92%
Clarity of Reports	89%
Effectiveness of Security Tips	95%

Features

The "Cryptocurrency Wallet Security Checker" includes the following key features:

- **Password Strength Analysis:** Evaluates password strength based on length, complexity, and entropy, providing recommendations for improvement.
- **Authentication Verification:** Checks for the presence and strength of Passwords, suggesting stronger options like hardware tokens.

- **Seed Phrase Protection Advice:** Guides users on secure seed phrase generation, storage, and recovery practices, emphasizing offline storage and avoiding phishing scams.
- **Phishing Detection:** Identifies and warns against phishing URLs using techniques similar to those employed by Google Safe Browsing API.
- **Software Update Reminders:** Notifies users of outdated wallet software, which may contain known vulnerabilities.
- **Secure User Interface and Reporting:** Provides a user-friendly interface with detailed security reports, explaining the risks and offering actionable advice.

5. Screenshots and Explanations

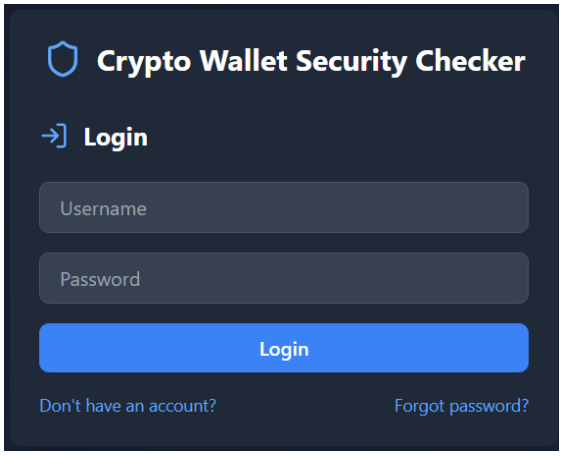

Figure 1: Login Interface

This screen provides users with secure access to their accounts. Users must enter their credentials before proceeding to the wallet security analysis.

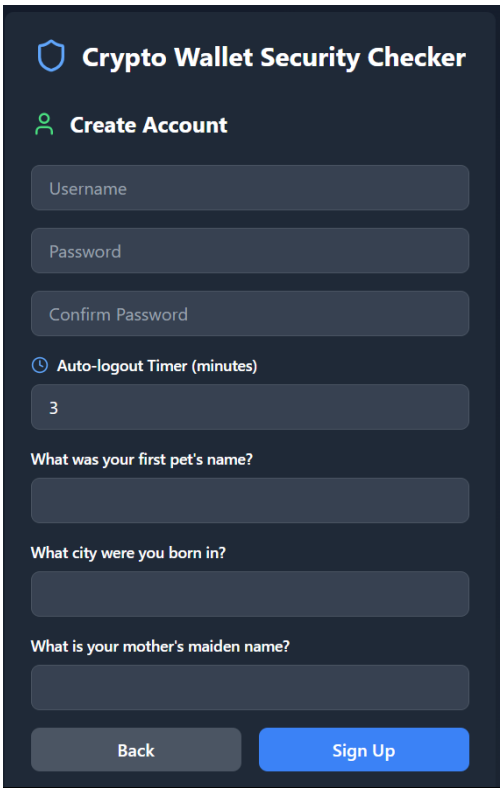

Figure 2: Create Account Interface New users can create an account with a secure password and 2FA settings to enhance security from the beginning.

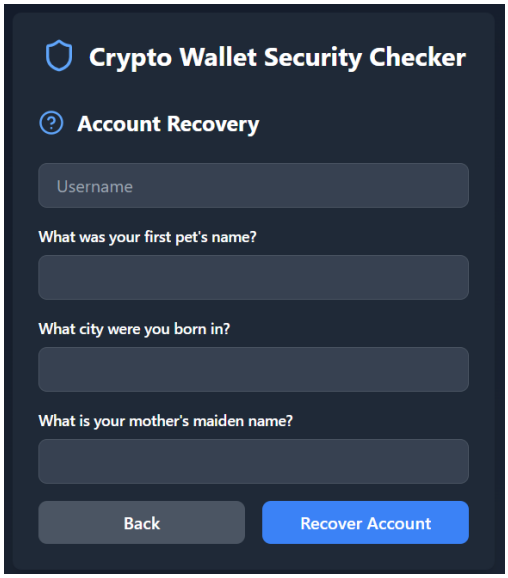

Figure 3: Account Recovery Interface

This screen allows users to recover their accounts using security questions, ensuring an additional layer of authentication.

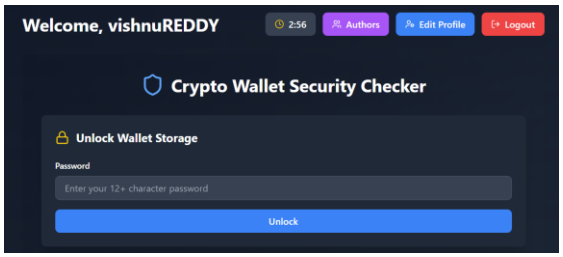

Figure 4: Wallet Storage Unlock Interface

Users must input a strong password to access their wallet storage, ensuring protection against unauthorized access.

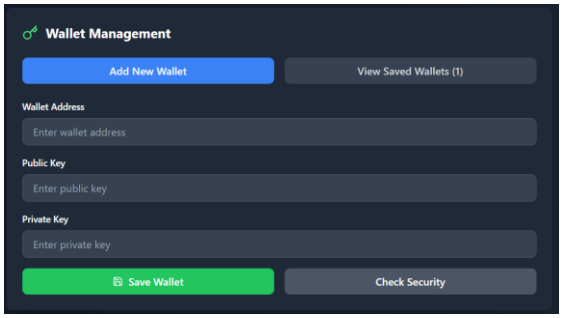

Figure 5: Wallet Management Interface

This feature enables users to add and manage multiple wallets securely while providing an overview of saved wallets.

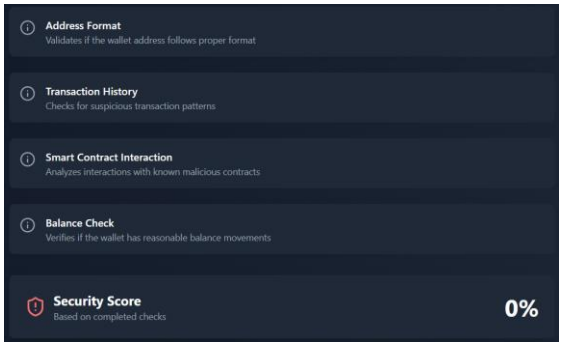

Figure 6: Wallet Security Interface The security assessment process includes transaction monitoring, smart contract analysis, and phishing detection. The security score is generated based on these factors.

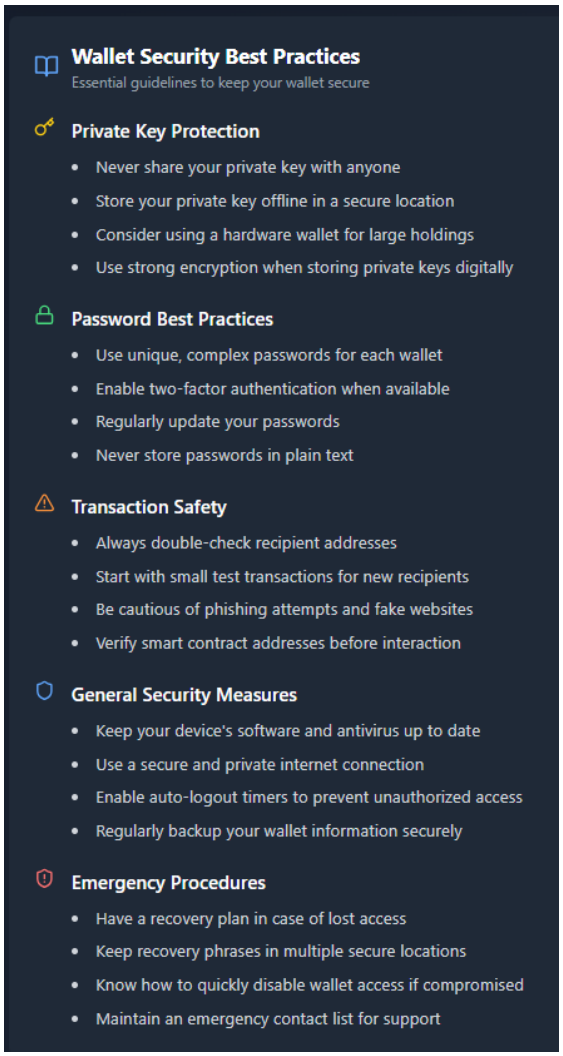

Figure 7: Wallet Security Practices Interface

Guidelines on best security practices for managing wallet credentials and preventing phishing attacks are displayed.

6. Conclusion and Future Work

the Cryptocurrency Wallet Security Checker effectively identifies security vulnerabilities and provides actionable recommendations to users. Future improvements include real-time threat monitoring, AI-based anomaly detection, and integration with hardware wallets. Expanding phishing detection capabilities and enhancing scalability will further strengthen its utility in securing cryptocurrency assets.

Acknowledgment

We extend our heartfelt gratitude to our mentors and faculty members for their invaluable guidance and support throughout this research. We are deeply thankful to Dr. S. Latha, our project supervisor, for her continuous insights and encouragement. Special thanks to Dr. S. Mohandoss and Ms. Y. Magana for their constructive feedback and expertise that helped shape this project. We would also like to acknowledge the Department of Computer Science and Engineering at Dr. M.G.R. Educational and Research Institute for

providing the necessary resources and an excellent research environment. Finally, we express our gratitude to our peers and families for their unwavering support and motivation throughout this project.

References

1. Bonneau, J., et al. "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies." IEEE Security & Privacy, 2023.
2. Antonopoulos, A. M. "Mastering Bitcoin: Unlocking Digital Cryptocurrencies." O'Reilly Media, 2020.
3. Moore, T., Clayton, R. "Examining the Impact of Website Take-down on Phishing." eCrime Researchers Summit, 2021.