Graph lock enhanced web security through Graphical passwords using Block chain

[1]A.BHAGYA SREE, [2]M MOUNIKA, [3]R ANJALI, [4]M AKHILA,[5]ATUFA SHAKOOR,[6] B ANUSHA,[7]MEHWISH FATHIMA

[1] Assistant Professor, Department of Computer Science and Engineering, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

[2,3,4,5,6,7] B.Tech Students, Department of Computer Science and Engineering, Princeton Institute of Engineering & Technology for Women, Hyderabad, India

Abstract:

In the digital age, securing user authentication is a critical challenge, especially as traditional text-based passwords continue to be vulnerable to phishing, brute-force attacks, and database breaches. This project proposes an innovative system called "Graph Lock", which combines the strengths of graphical passwords and block chain technology to create a robust and secure web authentication framework. Graphical passwords offer a more intuitive and memorable alternative to alphanumeric credentials, reducing the risk of weak or reused passwords while enhancing user experience. To ensure the integrity and security of stored credentials, this system leverages the decentralized and immutable nature of block chain. User-selected graphical password data is securely encrypted and stored across a block chain network, eliminating the risks associated with centralized password databases. Each login attempt is verified through smart contracts, ensuring trustless authentication and resistance to tampering or unauthorized access. The proposed system not only enhances security but also builds user trust by offering transparent and verifiable authentication records. "Graph Lock" represents a forward-thinking approach to user authentication, merging usability and advanced cryptographic security to protect against modern cyber threats in web applications.

I.INTRODUCTION

In today’s digital landscape, where cyber threats are increasingly sophisticated and frequent, securing user authentication has become a top priority. Traditional text-based passwords, though widely used, suffer from several vulnerabilities such as poor memorability, predictability, and susceptibility to brute-force attacks, phishing, and database leaks. Users often choose weak passwords or reuse them across platforms, making it easier for attackers to compromise accounts. As a result, there is a pressing need for more secure and user-friendly authentication mechanisms.Graphical passwords have emerged as a promising alternative, leveraging the human brain's superior ability to remember visual patterns over complex alphanumeric strings. By allowing users to select images, patterns, or positions as their passwords, graphical authentication improves memorability and reduces the likelihood of password-related errors. However, traditional graphical password systems still rely on centralized databases, making them vulnerable to data breaches and insider threats.To address these limitations, this project introduces "Graph Lock", a novel system that combines graphical password authentication with the security advantages of blockchain technology. Blockchain offers a decentralized, tamper-proof ledger where data is stored across a distributed network, making unauthorized access or modification nearly impossible. By storing encrypted graphical password hashes on a blockchain and utilizing smart contracts for authentication verification, the system ensures that no single point of failure exists.

This integration of graphical passwords and blockchain not only enhances web security but also increases transparency and trust in the authentication process. Users gain control over their credentials, and organizations benefit from a more resilient security framework. "Graph Lock" represents a significant step toward next-generation authentication systems that are both secure and user-centric.

II.LITERATURE SURVEY

Over the years, researchers and cybersecurity experts have explored various authentication methods to address the weaknesses of traditional password systems. Graphical passwords and blockchain technology have emerged as two promising areas in this regard. This literature survey reviews significant research contributions that support the development of a secure authentication system using graphical passwords integrated with blockchain.

1. Jermyn et al. (1999) – "The Design and Analysis of Graphical Passwords"

This early work introduced the concept of using graphical inputs, such as patterns on a grid (Draw-a-Secret method), for authentication. The study highlighted how graphical passwords offer better memorability compared to textual passwords.

Contribution: Introduced foundational graphical password schemes.

Limitation: Still vulnerable to shoulder surfing and brute-force attacks if not combined with other methods.

2. Biddle et al. (2012) – "Graphical Passwords: Learning from the First Twelve Years"This comprehensive survey analyzed various graphical password schemes, their

usability, and their vulnerabilities. It categorized schemes into recognition-based, recall-based, and cued-recall-based methods. Contribution: Provided insights into usability and security trade-offs in graphical password systems.

Limitation: Many schemes were theoretical or lacked robust implementation and security layers.

3. Bonneau et al. (2012) – "The Quest to Replace Passwords" The paper compared authentication systems based on usability, deployability, and security. It noted that while graphical passwords improve usability, they often lack strong security unless combined with other mechanisms.

Contribution: Provided comparative analysis of alternative authentication methods.

Limitation: Did not focus on decentralized or blockchain-based implementations.

4. Nakamoto, S. (2008) – "Bitcoin: A Peer-to-Peer Electronic Cash System"Although not directly related to authentication, this seminal paper introduced blockchain technology as a decentralized, secure, and transparent system, laying the foundation for blockchain-based applications in many domains.

Contribution: Introduced the blockchain concept.

Limitation: Focused on financial transactions, not identity/authentication use cases.

5. Kaaniche and Laurent (2017) – "Blockchain for Peer-to-Peer Confidential Storage"

This study explored how blockchain can be used to store data securely and privately, reinforcing the idea that user credentials can be stored on-chain in a decentralized and tamper-proof manner.

Contribution: Demonstrated blockchain’s potential for secure data storage.

Limitation: Did not address graphical authentication specifically.

III.EXISTING SYSTEM

In the current digital ecosystem, most websites and applications still rely on conventional text-based passwords for user authentication. These systems require users to create passwords using combinations of letters, numbers, and symbols, which are then stored in centralized databases. While commonly used, this method suffers from multiple drawbacks. Users often create weak, predictable passwords or reuse the same password across platforms, making them highly vulnerable to brute-force attacks, dictionary attacks, and phishing schemes. Additionally, centralized password storage is a significant security concern, as it presents a single point of failure—if the server is compromised, all user credentials are at risk. Although some platforms have introduced graphical password systems and two-factor authentication (2FA), these solutions are either limited in scope or fail to fully address the risks associated with centralized data storage and poor user practices. As a result, the existing systems do not provide sufficient protection against modern cyber threats.

IV.PROPOSED SYSTEM

To overcome the limitations of traditional authentication methods, the proposed system—Graph Lock—introduces an innovative approach that combines graphical passwords with blockchain technology for enhanced web security. Instead of relying on alphanumeric strings, users will select images, patterns, or positions as their password, which significantly improves memorability and reduces the chances of using weak or reused passwords. The selected graphical credentials are then encrypted and stored on a decentralized blockchain network, rather than a central server. This eliminates the single point of failure issue and ensures that the data cannot be tampered with or accessed by unauthorized users. Authentication is handled using smart contracts, which verify login attempts in a trustless and transparent manner. Blockchain's immutability and distributed ledger capabilities ensure that every action is securely logged, offering an additional layer of accountability and protection. This system not only enhances security but also improves user experience and builds trust through a more resilient and decentralized authentication framework.

V.SYSTEM ARCHITECTURE

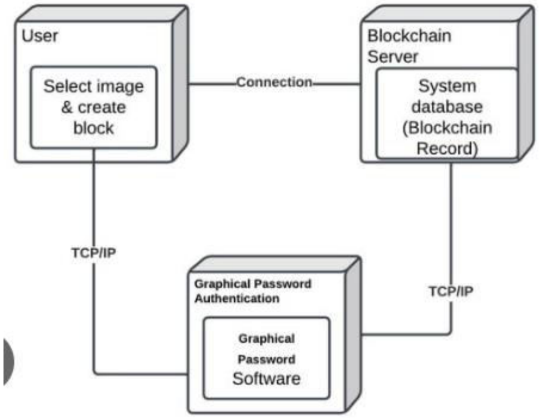
User
Select image & create block
Connection
Blockchain Server
System database (Blockchain Record)
TCP/IP
Graphical Password Authentication
Graphical Password Software
TCP/IP

Fig 5.1 System Architecture

The system architecture for identifying fake products using blockchain technology is designed to ensure transparency, security, and real-time verification of product authenticity. At the front-end, users interact with the application through a client browser interface built using HTML, CSS, and React.js. This user-friendly interface allows manufacturers to register products, distributors to update product movements,

VI.IMPLEMENTATION

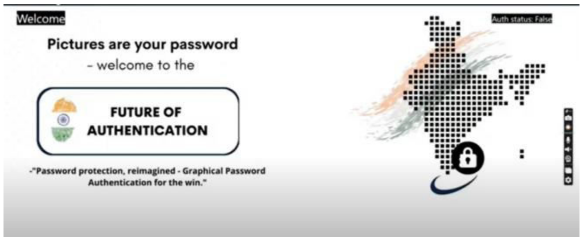
Welcome
Auth status: False
Pictures are your password
- welcome to the
FUTURE OF AUTHENTICATION
-"Password protection, reimagined - Graphical Password Authentication for the win."

Fig 6.1 Home page

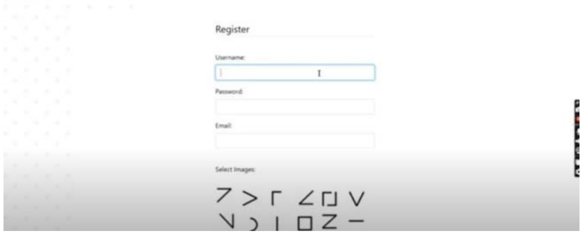

Fig 6.2 :Register page

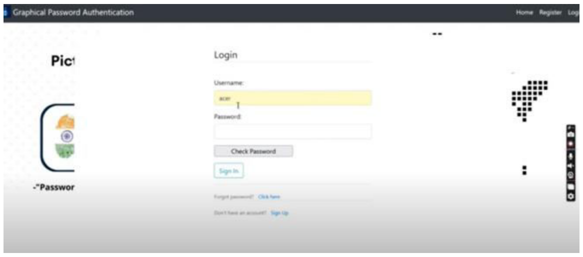
Graphical Password Authentication
Home
Register
Login
Username:
Password:
Check Password
Sign In
Forgot password? Click here
Don't have an account? Sign Up

Fig 6.3 Login page

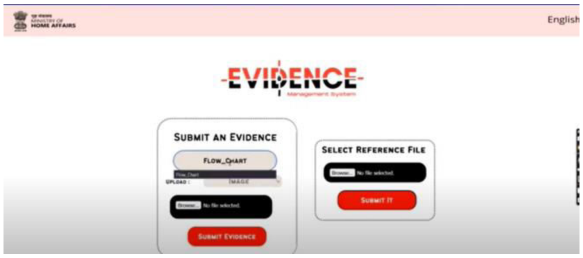

Fig 6.4 Evidence Page

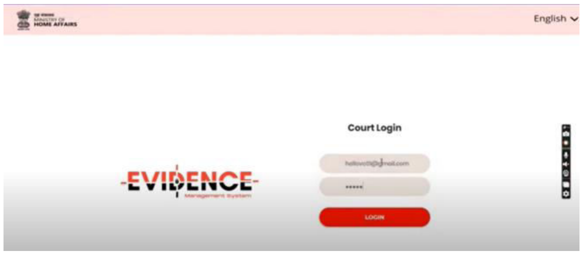

Fig 6.5 Court Login page.

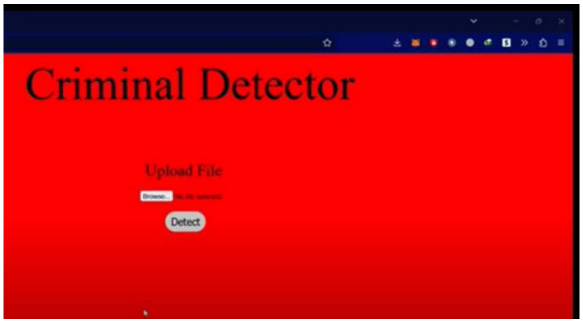

Fig 6.6 Criminal Detector page

VII.CONCLUSION

In conclusion, using blockchain technology to store and manage passwords is a secure and efficient method that makes it difficult for hackers to access. It also reduces the chances of users forgetting their passwords. The goal of this project is to develop a graphical password system that is resistant to shoulder surfing and can address the issues of weak passwords, vulnerability to dictionary attacks, and insufficient password complexity. The paper also explores blockchain-based protocols used in similar projects and aims to build a graphical password authentication system that improves security and execution.

VIII.FUTURE SCOPE

The integration of graphical passwords with blockchain technology in the proposed Graph Lock system opens up multiple avenues for future enhancements and real-world deployment. As cybersecurity threats continue to evolve, there is a growing demand for authentication mechanisms that are not only secure but also user-friendly and scalable. This project lays the foundation for such systems, with significant potential for further research and development.One of the key future directions is the implementation of multi-factor authentication (MFA) by combining graphical passwords with biometric data (such as fingerprint or facial recognition) and blockchain-based identity verification. This would significantly increase the overall security and make unauthorized access virtually impossible.Another promising area is the use of Decentralized Identity (DID) frameworks, which allow users to own and control their digital identities without relying on centralized authorities. By integrating DID with graphical authentication and blockchain, users can maintain complete control over their credentials while securely interacting with various platforms.The scalability of the system can also be improved by exploring Layer 2 blockchain solutions or using more efficient consensus mechanisms to reduce transaction costs and improve speed, making the system suitable for large-scale deployment in enterprises, e-commerce platforms, banking, and government services. Furthermore, a mobile application version of Graph Lock can be developed to increase accessibility and usability, especially in areas with limited desktop access. Offline authentication modes using secure local blockchain nodes could also enhance functionality in low-connectivity regions.

Lastly, integrating AI-driven security analytics can help detect unusual login behavior or image selection patterns, proactively identifying and mitigating threats. With advancements in blockchain interoperability, the system can eventually support cross-platform authentication across multiple blockchains and service providers.

IX.REFERENCES

[1] Pratima Sharma, Rajni Jindal, and Malaya Dutta Borah, “A Comparative Analysisof Consensus Algorithms for Decentralized Storage Systems,” IT Professional, IEEE.

[2] https://www.ijraset.com/research-paper/graphicalpassword-authenticationsystem5. A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, and P. Bhogle, ”Comparison of graphical Password authentication techniques,” International Journal of Computer Applications, vol. 116, no. 1, pp. 11–14, Apr. 2015.

[3] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems,”

International Journal of Human-Computer Studies, vol. 63, 2005.

[4] S. Chiasson, P. van Oorschot, and R. Biddle, “Graphical password authentication .

[5] M. S. Umar and Salim Istyaq, Encoding Passwords using QR Image for Authentication, IEEE Xplore Digit. Libr., 2016.

[6] Pratima Sharma, Rajni Jindal, and Malaya Dutta Borah, “A Comparative Analysisof Consensus Algorithms for Decentralized Storage Systems,” IT Professional, IEEE.

[7] https://www.ijraset.com/research-paper/graphicalpassword-authenticationsystem5. A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, and P. Bhogle, ”Comparison of graphical Password authentication techniques,” International Journal of Computer Applications, vol. 116, no. 1, pp. 11–14, Apr. 2015.

[8] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems,” International Journal of Human-Computer Studies, vol. 63, 2005.

[9] S. Chiasson, P. van Oorschot, and R. Biddle, “Graphical password authentication (recall-Based technique),” in European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007.

[10] M. S Umar and Salim Istyaq, Encoding Passwords using QR Image for Authentication, IEEE Xplore Digit. Libr., 2016.