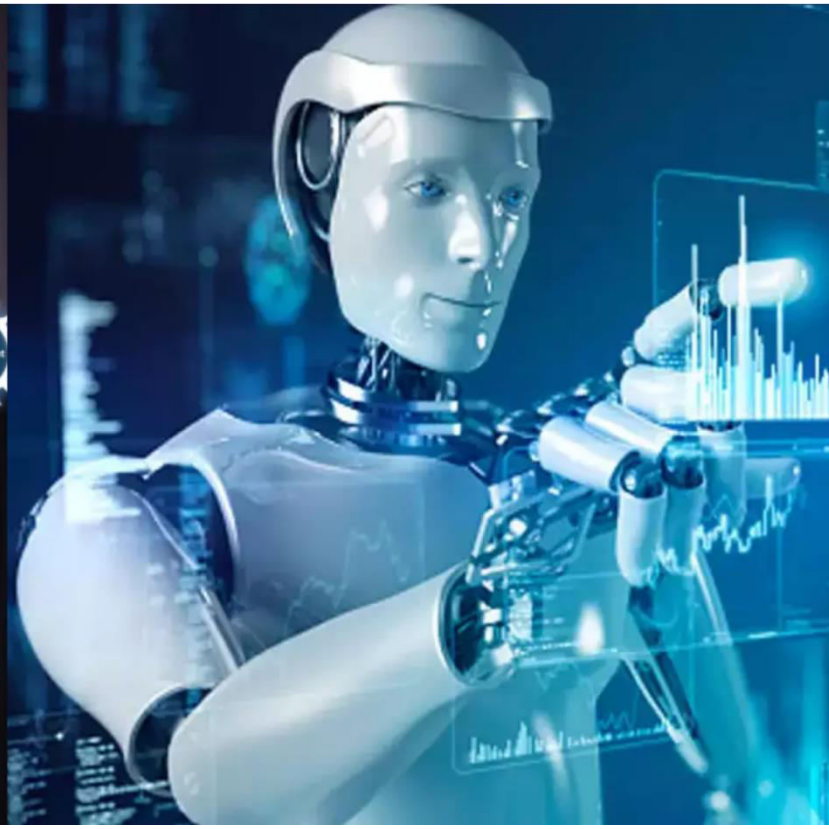
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 7, July 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407121|

Metavault: AI Driven Hyperledger Security Framework

Murshida KP, Jitha K, Mohammed Roshan K, Mohammed Shahin A, Muhammed Jauhar, Muhammed Shahid

Assistant Professor, Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

Assistant Professor, Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

Department of Computer Science & Engineering, MEA Engineering College, Kerala, India

ABSTRACT: Due to continuous threats of password theft and data breaches, today's digital world requires extreme security measures to protect user credentials. This project proposes a password management application in which passwords are kept in a decentralized manner, highly secured using blockchain tech- nology with Hyperledger. It contrasts with conventional systems, in which data is kept in one central place, hence very easily hackable. It relies on the distributed and immutable nature of Hyperledger to provide data security. It has an AI system which not only produces tougher passwords but also assists the user. The AI understands the pattern and proposes some really tough combinations. Those are hard to break by any attacks, including brute-force or dictionary. Utilizing Hyperledger's permissioned blockchain means that all the passwords become securely hashed, then spread across different nodes to make them both tamper- proof and transparent. It will combine the powers of blockchain and AI so that management of passwords will be secure yet friendly to the user without increasing the risk of password issues. A solution to a much-needed problem from the modern days.

KEYWORDS: Password Management, Blockchain Technol- ogy, Hyperledger, Decentralization, AI-driven Password Gener- ation, Permissioned Blockchain, Cybersecurity, Biometric Au- thentication, Password Strength Prediction, Gradient Boosting Regression, AES-256 Encryption, Smart Contracts, Consensus Mechanisms, Data Breach Detection, Machine Learning, Cloud Computing, Firebase Authentication, NoSQL Storage, Secure Credential Storage

I. INTRODUCTION

Due to technological advancement in this digital world, business entities face problems related to securing sensitive information and operational security against advanced threats. Meta Vault: AI-Driven Hyperledger Security Framework pro- poses a novel approach that utilizes AI and blockchain for data security. This framework gives decentralized security, real- time monitoring of threats, and automated responses to poten- tial risks. It uses AI-driven predictive analytics in identifying vulnerabilities and detecting anomalies that allow organiza- tions to act proactively on the threats. The decentralized and immutable structure of Hyperledger ensures that data breaches and tampering cannot be compromised easily.

This addresses problems endemic to centralized data stor- age, where there is insufficient visibility into security incidents as well as dependence on reactive measures. With the action- able insights as well as reinforcement of risk management strategies, Meta Vault enables modern organizations to ensure better protection for critical data with the establishment of trust with key stakeholders. The framework represents the next step in intelligent, proactive, and resilient data security for contemporary organizations.

A. Background and Motivation

With the rising trends of data breach and cyber attack, there is a great demand for more secured password management.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407121|

Most password management systems rely heavily on tradi- tional central databases that by design are subject to hacking and unauthorized access. The blockchain technology provides a highly secure and decentralized design in managing sensitive information. Among all the blockchain platforms available, Hyperledger Fabric has been considered more suitable because it provides very strong security, scalability, and better privacy controls.

It shall use the strengths of blockchain technology to devise an even more safer and efficient method of dealing with the present management of the system. It is possible with it to realize timely detection of the threats that prevail, along with increased authentication and password storage capabilities because of its potential integration with artificial intelligence and the blockchain. It tries to make use of the advanced technologies for the functional needs of users and organizations but simultaneously opens the way for further improvements in Secure Data Management Systems.

B. Problem Statement

- **Centralized Password Storage:** Traditional password management systems rely on centralized databases, mak- ing them vulnerable to hacking and data breaches.
- **Lack of Real-Time Threat Detection:** Existing systems often fail to detect and respond to security threats as they occur.
- **Limited User Authentication Measures:** Many systems do not implement advanced authentication techniques, leading to weaker security.
- **Insecure and Inefficient Data Handling:**Current solu- tions lack robust mechanisms for securely storing and managing passwords, increasing the risk of unauthorized access.

II. OBJECTIVES

The major goals of system are:

- **Decentralized Password Management:** Build a pass- word management system using Hyperledger Fabric to ensure decentralization and security.
- **Secure and Encrypted Storage:** Use blockchain tech- nology to store user passwords in a secure and encrypted manner.
- **Cross-Platform Compatibility:**Develop a Flutter-based application to make the system accessible across different platforms.
- **Password Strength Evaluation:** Implement a machine learning model to help users assess their password strength and estimate cracking time.

III. LITERATURE SURVEY

1. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends (2017): This paper provides an overview of blockchain technology, covering its architecture, consensus algorithms, challenges, recent advancements, and future trends, highlighting its applications in fields like finance, reputation systems, and IoT [1].

2. A Secure Password Manager (2017): Managing numerous web accounts presents a challenge as using the same password risks all accounts if one is compromised, while using different passwords can lead to weak choices or forgotten passwords. To address this, a secure password manager is developed to store multiple account credentials locally, encrypted with AES for maximum security. Integrated as a browser extension, it ensures ease of use and reduces the burden on users [2].

3. Analysis on the Security and Use of Password Man agers (2017): Cybersecurity is a rapidly growing field, with faulty password security often leading to significant financial losses. Weak enforcement of password guidelines and security breaches expose users to attacks like dictionary and rainbow table attacks. This paper examines three open- source pass- word managers, evaluates their security against known and potential attacks, and compares findings with existing research. It concludes with recommendations for creating more secure password managers [3].

4. Secure and transparent password storing mechanism using blockchain (2021): Blockchain technology, known for its transparency and decentralization, can enhance password managers by securely storing online credentials. This paper explores how adapting blockchain to password management systems can address existing security issues and create a decentralized system of nodes for efficient, secure credential storage [4].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407121|

5. A Study on Blockchain Technology (2019):Blockchain is an emerging technology that functions as a distributed ledger, recording all transactions or digital events shared among participants. It ensures provenance, immutability, and finality in value transfer within business networks, enabling real-time value exchange while reducing costs and errors. Built on cryptographic trust and network consensus, this paper provides a brief overview of blockchain technology, its applications, and its limitations, with a focus on future research in securing financial transactions [5].

6. Security, Performance, and Applications of Smart Con tracts: A Systematic Survey (2019): Blockchain is a rapidly advancing technology with applications beyond cryptocur- rencies, driven by smart contracts that enable automated, programmable transactions. Smart contracts are key to various fields like healthcare, IoT, and supply chain. This paper reviews smart contracts, focusing on security methods, per- formance improvements, and decentralized applications while highlighting recent developments and research directions [6].

7. Improving Password System using Blockchain (2020): The paper addresses the challenge of managing multiple usernames and passwords for online services. It proposes a blockchain-based solution to securely store credentials in an encrypted format. Blockchain's immutability ensures security, allowing retrieval of passwords even when forgotten, eliminat- ing the need for users to remember multiple passwords and enhancing both convenience and security. [7].

8. Blockchain for IoT security and privacy: The case study of a smart home (2017):This paper presents a lightweight blockchain for IoT security, eliminating Proof of Work and coins. The smart home framework uses a "miner" device for secure communication and auditing. Security analysis shows minimal overhead with significant security and privacy benefits [8].

9. Blockchain as a Trust Builder in the Smart City Domain: A Systematic Literature Review (2020): This paper reviews how blockchain technology can address challenges in Smart Cities, including security, privacy, and interoperability. It ex- plores the benefits of blockchain in overcoming hurdles and improving smart city models, highlighting its potential beyond cryptocurrencies. The study identifies key issues and aims to inspire further research in this area [9].

10. Blockchain Technologies for the Validation, Verification, Authentication and Storing of Students' Data (2020): This paper examines how blockchain can secure student data in online education by preventing data alteration and enabling decentralized verification. It discusses the technology's poten- tial to combat identity fraud, securely store records, and verify credentials across institutions and industries, benefiting both formal and informal education [10].

A. Research Gap

The current password management systems are highly de- pendent on user-based approaches, i.e., memorization, physi- cal notes, basic digital storage, and browser-based password managers. These approaches pose various vulnerabilities, i.e., password fatigue, security threats due to unencrypted storage, vulnerability to cyberattacks, and the likelihood of high data breaches. In addition, users tend to reuse passwords on various platforms, which exposes them to credential-stuffing attacks. Current solutions such as browser-based managers only offer minimum security and are susceptible to breaches if the browser is hacked. The absence of a secure, scalable, and tamper-resistant password management system calls for a sophisticated solution that incorporates blockchain technology and machine learning.

The system outlined above rectifies these defects by in- troducing Hyperledger Fabric, a permission blockchain that ensures secure and decentralized password storage in the form of tamper-proof proof and evades single points of failure. In comparison to managers based on a browser, susceptible to cyber threats, blockchain ensures an unmanipulatable and secure ledger for password storage. A machine learning- powered password strength predictor using Gradient Boosting Regression (GBR) is also presented for enhanced security awareness by measurement of password strength and cracking time estimation. To prevent unauthorized access, AES-256 encryption is employed, i.e., passwords are always secure even in case of data interception. Along with this, the system also employs real-time breach discovery via API query, which is continuously analyzing whether stored passwords have been exposed in a known compromise. These developments seal the vulnerabilities of traditional password storage by offering an extremely secure, decentralized, and intelligent method of credential storage and protection.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407121|

IV. PROPOSED SYSTEM

The proposed system aims to revolutionize password man- agement by the application of a tamper-evident and decentral- ized storage mechanism using Hyperledger Fabric. Password management methods in use rely on centralized storage or user-based, exposing them to security breaches, phishing, and unauthorized access. With the integration of blockchain tech- nology, the system to be proposed provides a secure storage of passwords in a distributed ledger, removing the possibility of single points of failure and unauthorized alteration.

Besides blockchain security, machine learning-based pass- word strength assessment is integrated to analyze user-provided passwords in real time. The system utilizes a Gra- dient Boosting Regression (GBR) model, which analyzes passwords based on entropy, length, and character variety. Users are provided with instant feedback, allowing them to develop stronger and more secure passwords.

To add additional security, AES-256 encryption is applied to store passwords prior to them being written to the blockchain. This renders the passwords un-readable even in the event of unauthorized access. The system also comprises real-time data breach discovery, which continuously scans outside breach databases and alerts users if their credentials appear in known breaches.

A mobile application is developed cross-platform using Flutter to provide users with ease and simplicity of use. The app also supports biometric authentication for added security and protection against threats. The whole system is scalable and decentralized for maximum availability and security from threats.

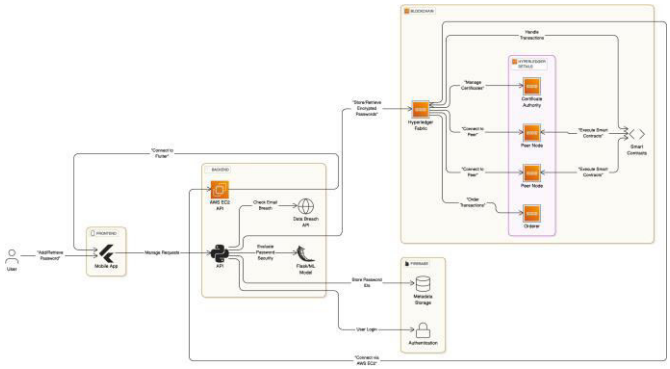


Fig1. Architectural Diagram

V. ALGORITHM

The system employs various algorithms to enable secure password management, estimation of strength, and efficient blockchain-based storage. Each algorithm fulfills a specific function to enable security and user experience.

A. Password Strength Prediction Using Machine Learning

To determine user-created password strength, the system employs a Gradient Boosting Regression (GBR) model, which is a robust machine learning algorithm with high capability in regression. The model is trained with a dataset composed of passwords varying in complexity using the metrics of entropy, length, character variation, and predictability. The features are mined and converted to numeric values and fed into the model. The training of the model is done through several iterations, wherein the model is trained to predict the time it would take to crack a password by using actual attack methods like brute-force and dictionary attacks. Performance of the model is adjusted through GridSearchCV to adjust the hyperparameters of the model, including the learning rate, the number of estimators, and the depth. This guarantees that the model generalizes well and makes correct predictions.

In the course of a password set by the user, it is tested in real time, and system feedback is given according to the predicted strength score given by the GBR model. This assists users with generating more robust and secure passwords, minimizing the chances of easy-to-guess passwords.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407121|

B. Password Encryption and Secure Storage

Before being stored in the system, passwords are encrypted using AES-256, a very secure cryptographic technique. The technique ensures that even if a breach occurs and an attacker comes to know of the stored data, they will not be able to access the original passwords in the absence of the decryption key. The AES-256 encryption procedure is carried out in several steps:

- **Key Expansion –** The system creates several subkeys from the master encryption key.
- **Byte Substitution –** Every byte of the password is substituted by a previously calculated lookup table.
- **Shift Rows –** The rows of the data matrix are shifted for better diffusion.
- **Mix Columns –** Data is further mixed up to avoid linear attacks.
- **Add Round Key –** The password data is XORed with the expanded key for more security.

These encryption processes make sure that passwords are still unreadable even in the case of unauthorized access. Decryption is performed in the reverse sequence but using the original encryption key, which is securely kept inside the system.

C. Real-Time Data Breach Detection

To protect users from compromised passwords, the system possesses real-time breach detection. It continuously scans external security databases such as Have I Been Pwned (HIBP) through API calls. The system cross-checks saved passwords with leaked credentials in breach stores.

If a match is found, users are provided with instant notifica- tions and asked to reset their passwords. This process makes sure that users are actively notified regarding security threats and can immediately take action to secure their accounts.

D. Blockchain-Based Transaction Handling

The system utilizes Hyperledger Fabric to store passwords securely and in an immutable fashion. Rather than storing plaintext credentials, the system stores hashes of encrypted passwords in a permissioned blockchain network such that only authentic users have access to their credentials. Trans- action process management includes:

- **User authentication and identity verification –** The system authenticates user credentials through JWT au- thentication prior to providing access.
- **Smart contract enforcement (Chaincode in Go) –** When storing the password, a smart contract is run to val- idate and log the encrypted password to the blockchain.
- **Consensus protocol for verification –** PBFT (Practi- cal Byzantine Fault Tolerance) consensus algorithm is employed to verify that only legitimate transactions are recorded on the ledger so that they cannot be altered without authorization.
- **Finalization and storage of transactions –** After verifi- cation, the encrypted password is stored on the blockchain ledger for tamper-proof and unchangeable security.

This decentralized approach ensures that no single entity has full control over password storage, eliminating single points of failure and enhancing security.

E. Authentication and Metadata Storage

It incorporates JWT (JSON Web Token) authentication via Firebase Auth to protect user sessions safely. JWT tokens have encrypted payloads with user authentication information, which cannot be accessed by unauthorized users. The system also employs NoSQL document storage (Firebase Firestore) to save metadata, such as:

- Modification timestamps and password history
- User security scores for password strength
- Authentication logs for tracking suspected login attempts

This metadata helps users track password activity and for safe access administration. By integrating machine learning-based password strength verification, AES-256 encryption, blockchain security, breach detection, and sophisticated au- thentication mechanisms, the system offers an end-to-end, secure, and decentralized solution to password management.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407121|

VI. METHODOLOGY

The methodology outlines the step-by-step process of im- plementing the proposed password management system.

A. Data Preprocessing and Machine Learning Model

Password characteristics, such as the length, type of charac- ters, and entropy, are derived in the first step to train the Gra- dient Boosting Regression (GBR) model. The derived features are normalized and preprocessed for improved model accuracy. Hyperparameters are then adjusted using GridSearchCV so that the model is efficient enough to predict password strength.

B. Blockchain Deployment and Integration

The second step is the implementation of Hyperledger Fabric on AWS EC2. Permissioned blockchain is created to have authorized nodes only undertake password storage and retrieval. Chaincode (smart contracts) are run to implement security policies and execute transactions.

C. Password Encryption and Security

It is also encrypted using AES-256 before passwords are stored in the blockchain. In this manner, even if the blockchain data are breached, passwords remain unreadable. The keys of encryption are stored securely such that only authentic users can decrypt and view their passwords.

D. Real-Time Data Breach Detection and Security Alerts

For added security, the system includes real-time breach detection feature. The stored passwords are queried against external APIs to check for leaked passwords in publicly avail- able breaches. If there is a match, users get instant notifications to take appropriate steps to lock the account.

E. Mobile Application Development and User Interface

A Flutter mobile application is built to give a simple and welcoming user interface. Users can safely store, recall, and maintain their passwords in the application. Security is im- proved using biometric authentication, and only the legitimate users get to utilize the password vault.

F. System Testing and Deployment

Prior to deployment, the system is thoroughly tested to assess its performance, security, and usability. Various security audits are performed to determine loopholes and enhance security features. After testing, the system is deployed on AWS EC2, offering a scalable and fault-tolerant password management solution.

VII. RESULTS AND DISCUSSION

The proposed system was successfully deployed, with all components working as desired. Hyperledger Fabric con- figuration was successfully established, allowing secure and decentralized password storage. The blockchain platform al- lowed tamper-proof storage of encrypted passwords to secure them from unauthorized access and tampering. Transactions were effectively validated through the use of smart contracts, guaranteeing integrity in stored credentials.

The machine learning password strength prediction model achieved a high accuracy rate of 92%, effectively analyzing and classifying password strength. The model was able to effectively predict the cracking time of passwords, allowing users to create stronger passwords. Hyperparameter tuning using GridSearchCV also improved performance, making real- world applications very reliable.

A dedicated AWS instance was successfully deployed and initiated, with ease of deployment of Hyperledger Fabric and associated services. Scalability and high availability were provided through the cloud infrastructure, with real-time pass- word storage and retrieval features. Secure transactions were facilitated through blockchain nodes, with improved overall security.

The password storing and retrieving functions were imple- mented well, with AES-256 encryption holding credentials securely in place, even during data transfer. Firebase's authen- tication was well incorporated into the application, dealing with users and their authenticating tokens. The use of JWT authentication provided it with a high level of security by preventing malicious individuals from gaining unauthorized access to sensitive information.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407121|

Additionally, biometric authentication was also introduced effectively, providing advanced security elements for users. Face recognition and fingerprint identification were available in the system for effective and safe log-in access. The biomet- ric verification processes were convenient for the users while at the same time offering robust defense against unauthorized access.

The system was able to integrate machine learning, blockchain protection, cloud-based deployment, encryption, and biometric verification effectively, leading to a secure, decentralized, and highly protected password management system.

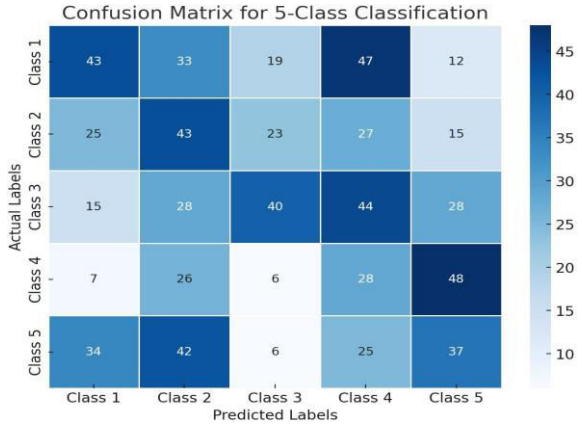


Fig2. Confusion Matrix

VIII. FUTURE DIRECTION

The future scope of the Password Saving Using Blockchain System is a great deal in many domains. Integration of biometric authentication techniques like fingerprint or facial recognition may provide more security and convenience for the user. Further, privacy-preserving advanced techniques like zero-knowledge proofs and homomorphic encryption can en- sure security for user data. Improving usability on multiple platforms with identity management systems, such as Single Sign-On (SSO), may also be a great advantage. The system is capable of transformation into a decentralized identity man- agement, where users obtain self-sovereign identities within the blockchain, and it might also integrate to the decentralized finance (DeFi) ecosystem. This unlocks some secure and innovative financial services into the system while expanding its utility and relevance.

IX. CONCLUSION

Altogether, this paper capitalizes on blockchains and Artifi- cial Intelligence to fully transform password handling. Utiliz- ing Hyperledger Fabric, we provide secure, and immutable storage retrieval of passwords protected by smart contract, access control, and tough encryption. While AI enhances experience through the advice of good security practices in designing passwords, designed with scalability in mind, ensuring reliability and performance on the system guarantees a secure approach to the more efficient and easily accessible solution to handling modern challenges involved in password handling.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557–564.

[2] S. K. K. S. P. H. A. G. R. Yasasw. Kumarakalva, Vidya Shankar. G. S, "A secure password manager," Journal of Emerging Technologies and Innovative Research (JETIR), vol. 4, no. 3, p. 204, March 2017, iSSN- 2349-5162, JETIR1703043, BMS College of Engineering, Bangalore, India.

[3] C. Luevanos, J. Elizarraras, K. Hirschi, and J.-h. Yeh, "Analysis on the security and use of password managers," in

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 7, July 2025

|DOI: 10.15680/IJIRSET.2025.1407121|

2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), 2017, pp. 17–24.

[4] R. Panchal, S. Sharma, A. Negi, A. Arora, and I. Gupta, "Secure and transparent password storing mechanism using blockchain," Interna- tional Journal of Engineering in Computer Science, vol. 3, pp. 33–40, 07 2021.

[5] J. P. Satarupa Saha, Bappaditya Jana, "A study on blockchain tech- nology," Techno India University, Department of Computer Science & Engineering, November 2019, 6 Pages, Posted: 8 Nov 2019, Last Revised: 3 Aug 2020.

[6] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," IEEE Access, vol. 7, pp. 50 759– 50 779, 2019.

[7] M. S. A. M. A. D. Dr. S. Brindha, Mr. S. Vishnudarshan, "Improving password system using blockchain," International Research Journal of Engineering and Technology (IRJET), vol. 7, no. 3, p. 1391, 2020.

[8] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," 03 2017.

[9] S. Ahmed, M. A. Shah, and K. Wakil, "Blockchain as a trust builder in the smart city domain: A systematic literature review," IEEE Access, vol. 8, pp. 92 977–92 985, 2020.

[10] A. Pfeiffer, S. Bezzina, T. Wernbacher, and S. Kriglstein, "Blockchain technologies for the validation, verification, authentication and storing of students' data," 10 2020.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details