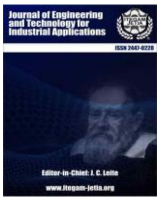
Journal of Engineering and Technology for Industrial Applications

ISSN ONLINE: 2447-0228

ITEGAM-JETIA

Manaus, v10. n.50, p. 230-237. November/ December., 2024.
DOI: https://doi.org/10.5935/jetia.v10i50.1433


Journal of Engineering and Technology for Industrial Applications
ISSN 2447-0228
Editor-in-Chief: J. C. Leite
www.itegam-jetia.org

RESEARCH ARTICLEOPEN ACCESS

VAULTGUARD: THE ADVANCED KEYLESS SECURITY SYSTEM

Dr. Yogita Mane [1], Dr. Neeta Patil[2], Akshay Agrawal[3], Sanketi Raut[4], Vishal Shinde[5]

[1,3,4] Department of Information Technology, Universal College of Engineering, University of Mumbai, Vasai
[2,5] University of Mumbai, Mumbai.

[1]https://orcid.org/0000-0002-7097-2193, [2]http://orcid.org/0009-0003-1532-3996, [3]http://orcid.org/0000-0002-8722-7181, [4]https://orcid.org/0000-0002-7097-2193, [5]https://orcid.org/0009-0009-3256-3012,

Email: yogita.ydmane@gmail.com, npat78691@gmail.com, akshay1661@gmail.com, sanketiraut28@gmail.com, mailme.vishalshine@gmail.com

ARTICLE INFO

Article History
Received: November 28, 2024
Revised: November 30, 2024
Accepted: December 10, 2024
Published: December 31, 2024

Keywords:
2 Factor Authentication,
WebAuthn,
Biometric Recognition,
Keyless Vault,
FIDO2.

ABSTRACT

The VaultGuard is a cutting-edge password management solution designed to enhance security, convenience, and user experience. A full-featured research work named VaultGuard is developed to assist users in safely creating, organizing, and storing strong passwords for a variety of online accounts and programs. This paper offers a wide range of features, including secure storage for multiple encrypted passwords using AES256 on cloud, Random key generation algorithm for creating an advanced password, updating user password timely, and a user-friendly dashboard for managing and organizing login information. The system provides a seamless registration process using Fast Identity Online 2 algorithm (FIDO2) with Web Authentication (WebAuthn) component, allowing users to securely login without needing any password. To further enhance security, the research paper employs AES256 Algorithm to safeguard stored passwords, protecting them from unauthorized access and data breaches. The system also proactively monitors the age of passwords and sends SMS and email notifications to users when their passwords are older than a predetermined time period, such as a month, prompting them to update their passwords for added security. By combining the convenience of password management with authentication, strong encryption, and proactive password monitoring, the VaultGuard sets a new standard for secure and user-friendly password management systems, effectively addressing the shortcomings of traditional methods with 97.66 % accuracy and 98.63% precision.

I. INTRODUCTION

In today's digital era, effective password management is crucial for ensuring online security and privacy. The VaultGuard Research paper is a comprehensive software solution designed to help users securely store, organize, and generate strong passwords for their various online accounts and applications. The VaultGuard enables users to store and manage their login credentials for different websites and services in a centralized, encrypted database. It requires a Passkey to access the stored passwords, making it more convenient and secure than memorizing multiple passwords [1], [2].

A Password-Based Authentication System Based on the CAPTCHA [3], represents Artificial Intelligence (AI) inspired security methods needed to secure communications in the era of quantum computing. The VaultGuard is a secure storage component that protects the user's sensitive information using strong encryption techniques [4]. This ensures that, even if the vault is compromised, the stored passwords remain secure and unreadable. The research paper offers a functionality to automatically create random passwords with a minimum length of 8-20 characters using a combination of uppercase letters, lowercase letters, 0-9 digits, and special symbols. It also displays the time required to crack the password by a supercomputer, few methods like Brute Force Attack, Dictionary Attack, Rainbow

Tables etc. can be used providing an estimate of its strength and use cases as mentioned in below Table 1 [5].

Table 1: Comparative Analysis of Different Password Cracking Algorithms.

Algorithm	Method	Strengths	Use Cases
Brute Force	Exhaustive Search	Guaranteed to find the password; simple implementation	Recovering short or weak passwords.
Dictionary Attack	Wordlist Matching	Fast; effective against weak passwords.	Cracking user-chosen weak passwords.
Rainbow Tables	Hash Lookup	Reduces time for cracking hashes; requires less computation than brute force.	Cracking stored hashed passwords.

Source: Authors, (2024).

To promote better password practices, the research paper includes functionality to monitor password age. If a user's password is older than 1 month, the server sends an email and an SMS notification to remind the user to update their password [6]. The VaultGuard Research paper is a robust and feature-rich solution for safeguarding sensitive login information, reducing the risk of data breaches, and promoting better password practices. It combines convenience, security, and advanced features to provide a comprehensive password management experience for users.

I.1 OBJECTIVES

The objectives of proposed research work are as follows.

- **To Implement Passwordless Authentication System:** Utilize FIDO2 with WebAuthn component standards to provide a secure, passwordless login system that mitigates the risks associated with traditional password-based authentication methods.
- **To provide Secure Password Storage:** Employ AES 256-bit encryption to ensure the secure storage of user-generated passwords within a MongoDB database, protecting sensitive user information from unauthorized access and data breaches.
- **To Automate Password Manager:** Integrate an automatic password generator that not only creates strong, randomized passwords combining uppercase letters, lowercase letters, 0-9 digits, and special symbols but also informs users about the estimated time required for this password to be cracked by a supercomputer.
- **To provide Proactive Security Notifications:** Develop a system that actively monitors the age of stored passwords and automatically notifies users via email and SMS when passwords need updating, thus maintaining high security standards over time.
- **To enhance User Experience:** By employing NodeJS and EJS, deliver a responsive, user-friendly interface that simplifies user interactions while maintaining high performance and security.

The overarching objectives of this research paper are to provide a comprehensive solution that not only secures user data but also enhances usability and promotes better password hygiene among users. This initiative is aligned with current trends in cyber security, aiming to reduce cyber risk through innovative technological advancements.

I.2 LITERATURE REVIEW

The study [1] presents "Building and Examining a Watchword Store that Impeccably Stows away Passwords from itself called SPHINX", which remains secure indeed when the secret word director itself has been compromised. In SPHINX, the data put away on the gadget is hypothetically autonomous of the user's ace watchword. Besides, an assailant with full control of the gadget, indeed at the time the client interacts with it, learns nothing about the ace secret word – the secret word is not entered into the gadget in plaintext frame or in any other way that may spill data on it.

In this inquiry about work [2], the creators dive profoundly into the offline word reference assaults on the database of passwords (PW) or indeed hashed PW are harmed as a single server break-in leads to numerous compromised PWs. In this respect, utilizing Physical Unclonable Capacities (PUFs) to increment the security of PW chief frameworks has been as of late proposed. Utilizing PUFs permits supplanting the hashed PW with PUF reactions, which give an extra equipment layer of security. In this way, indeed with getting to the database, an enemy ought to have physical control of the PUF to discover the PWs.

A Password-Based Confirmation Framework Based on the CAPTCHA, as portrayed [3], speaks to Manufactured Insights (AI) motivated security strategies required to secure communications in the period of quantum computing. This article presents a challenge-response password-based verification framework based on the Totally Mechanized Open Turing test to tell Computers, People Separated (CAPTCHA) AI difficult issues. In this framework, a server sends a challenge content to a client, and at that point the client produces an arbitrary picture and mixes the challenge content inside this irregular picture utilizing his watchword. At that point the client sends the produced picture to the server. The server extricates the challenge content from the sent picture utilizing his duplicate of the client's secret word. If the extricated challenge content is the same as the sent challenge content, at that point both the client's and the server's duplicates of the secret word coordinate and the client is authenticated.

The work [4] investigates the interesting world of propositions to handle the issue of watchword spillage of prevalent websites like Linked-In, Adobe, Gmail, Yahoo, eHarmony, etc. by utilizing energetic watchword arrangement and improved hash Calculation. Here, a calculation is created that will produce watchword arrangements powerfully depending on the recurrence of characters. Time complexity is computed, and it is found that the calculation works quickly. Since the calculation makes watchword arrangements powerfully, it will be intense for the aggressor to figure the characteristics of the secret word database.

The investigate study [5,6] basically centers on reinforcing the passkey section convention and securing the gadgets against detached listening in and dynamic Man-in-the center (MITM) assaults in both Bluetooth Essential Rate/Enhanced Information Rate (BR/EDR) and Bluetooth Moo Vitality (Bluetooth LE). This strategy can be utilized for any gadget which employs the passkey passageprotocol.

The work [7],[8] leads to key experiences almost the trouble of supplanting passwords. Not as it were does no known plot come near to giving all craved benefits: none indeed holds the full set of benefits that bequest passwords as of now give. In specific, there is a wide range from plans advertising minor security benefits past bequest passwords, to those advertising critical security benefits in return for being more exorbitant to send or more troublesome to utilize. This research paper concludes that numerous scholarly recommendations have fizzled to pick up footing since analysts once in a while consider a adequately wide run of real-world limitations.

I.3 EXISTING SYSTEMS

The current landscape of password management and authentication systems is characterized by a reliance on traditional password-based mechanisms [1-10], which pose numerous security challenges. Despite advancements in cryptographic practices, many systems continue to depend on passwords that users often find difficult to manage and remember, leading to compromises in security practices such as the reuse of passwords across multiple sites.

The introduction of two-factor authentication (2FA) [11] has provided an additional layer of security; however, it often adds complexity to the user experience and does not eliminate the fundamental vulnerabilities associated with password theft or loss. Moreover, many 2FA implementations remain susceptible to phishing and man-in- the-middle attacks, which can intercept or replicate the second fator[12].

Password managers have become popular for storing and generating secure passwords, yet they also concentrate risk by storing multiple passwords in a single location, often protected by a single master password [13]. Every credential that is stored is vulnerable if the master password is hacked. Furthermore, these systems do not inherently encourage or enforce strong password creation, nor do they typically address the issue of password aging, leaving users with potentially vulnerable accounts over time.

Recent developments in the field have seen the adoption of password-less authentication methods, such as biometrics and hardware tokens, which offer improved security by eliminating the need for stored secrets that can be stolen or lost. However, these technologies often require additional hardware or specific environmental conditions, which can limit their accessibility and general usability.

In summary, while existing systems have made strides towards enhancing security and user convenience, significant challenges remain, particularly in terms of security robustness, user experience, and accessibility. These challenges underscore the necessity for innovative solutions like “VaultGuard,” which seeks to address these gaps through the integration of advanced encryption, password-less authentication, and proactive security measures.

I.4 LIMITATION ON EXISTING SYSTEM

The limitations of the existing systems are as follows;

- Password managers that store user data in a centralized server can pose a risk if the server is compromised or becomes unavailable [13].
- Some password managers may not support all operating systems, browsers, or devices, which can limit accessibility for users working across multiple platforms.
- Synchronization issues may arise when using password managers across multiple devices, leading to inconsistencies or delays in accessing passwords.
- Despite the convenience of password managers, some users may find them complex or intimidating to set up and use, which could hinder adoption and usage.
- While some password managers are free, others may require a subscription, which can be a barrier for users who prefer a free solution or are unwilling to pay for additional features [12].
- If a user's master password is compromised, all the stored passwords within the password manager become vulnerable. Implementing additional security measures, such as two-factor authentication, can help mitigate this risk, but it remains a limitation of password-based systems [13].

I.5 PROBLEM STATEMENT

In today's digital age, managing multiple online accounts with unique and robust passwords has become a challenging task for individuals and organizations. Users often struggle to remember complex passwords or resort to using the same passwords across multiple websites, which can lead to security vulnerabilities. Traditional password-based authentication systems are susceptible to various threats, such as weak passwords, phishing attacks, and data breaches. Existing password management systems may not offer adequate protection against unauthorized access, leaving sensitive data vulnerable.

Users often lack the knowledge and resources to create strong, unique passwords for their accounts, further compromising their security. Creating and managing complex passwords can be time-consuming and cumbersome, leading to frustration and decreased user adoption. Ensuring the security of stored passwords is a significant challenge, and data breaches can have severe consequences for both individuals and organizations.

To address these challenges, the VaultGuard aims to develop a comprehensive and secure password management solution that incorporates a robust password generator, a secure password vault, and encryption algorithms to safeguard sensitive information. By offering a user-friendly and highly secure password management system, the study aims to improve password security, reduce the burden of managing multiple passwords, and enhance overall digital security for users.

II. PROPOSED SYSTEM

To address the limitations identified in existing password management and authentication systems, “VaultGuard” introduces a comprehensive solution that emphasizes security, usability, and proactive management. The proposed system integrates several key innovations and improvements over traditional methods:

Passwordless Authentication using FIDO2 with WebAuthn component: “VaultGuard” utilizes the FIDO2 standard to enable passwordless authentication. This method significantly reduces the risk of password-related breaches by eliminating the need for users to remember and manage traditional passwords, thus also decreasing vulnerability to phishing and brute-force attacks.

AES 256-Bit Encryption: All passwords generated or stored within the system are encrypted using the Advanced Encryption Standard (AES) with a 256-bit key, currently the gold standard in encryption. This ensures that even if data is intercepted, it remains protected against unauthorized access.

Automated Random Password Generator: The system includes a feature to automatically generate complex passwords using a mix of uppercase letters, lowercase letters, numbers, and symbols. It also provides an estimate of how long different algorithms or techniques would take to crack each password, helping users understand their password strength better..

Proactive Password Aging and Notification System: "VaultGuard" actively monitors the age of stored passwords and notifies users via email and SMS when it is time to update their passwords. This feature helps maintain high security standards by ensuring that passwords are regularly updated and not left vulnerable over time.

User-Friendly Interface: The application is developed using NodeJS for the backend and Embedded JavaScript Templates (EJS) for the frontend, providing a smooth and responsive user experience. This approach allows for quick interactions and a more intuitive user interface, which is accessible even to users with minimal technical expertise.

By combining these features, "VaultGuard" not only provides a more secure method of managing passwords but also enhances the overall user experience, making it a versatile and robust solution in the domain of digital security.

The following Fig. 1 shows a multi-layered architecture which follows the Advanced Password Manager to ensure security, scalability, and performance. The system comprises a client-side interface built using modern web technologies, a password generator module, a password vault backed by AES 256 encryption, WebAuthn integration for password less login, and automatic password aging notification functionality. The system architecture also includes a robust database layer using MongoDB for storing encrypted user passwords. The application server handles requests, processes user data, and communicates with the database to ensure seamless user experience. The system architecture is designed to be modular, secure, and scalable, making it an ideal solution for managing passwords and enhancing digital security in the modern era.

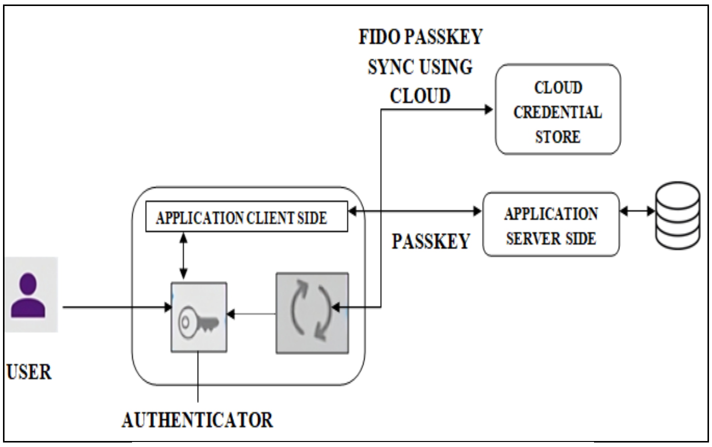


Figure 1: VaultGuard System Architecture.
Source: Authors, (2024).

Client Side: represents the user interface that users utilize to engage with the system; this is usually a web browser or an application.
Web Server (Backend): Acts as the intermediary between the client-side interface and the database. It hosts the application logic, including API endpoints for handling user requests.
Application Logic (API): Handles user authentication, password management, and notification services. It includes modules for WebAuth authentication, password generation, and expiry notification.
MongoDB Database: Stores user data, including user information (name, email, mobile number) and passwords. It consists of collections for users and passwords, enabling CRUD operations.

The arrows indicate the flow of data and interactions within the system: Users interact with the client-side interface, making HTTP(S) requests. The web server receives these requests and forwards them to the application logic. The application logic processes the requests, interacts with the MongoDB database as needed, and sends responses back to the client. Database queries are executed to read or modify user data stored in the MongoDB database. The notification service may also interact with external services (e.g., email and SMS gateways) to send notifications to users.

The advantages of the proposed system are that it provides password-less login having secure password storage. It also generates random passwords and provides password expiry reminders to the users. It also provides Better Security Compliance consisting of Multi-factor Authentication.

III. METHODOLOGY

As shown in Fig. 2, when the user tries to sign in it first checks whether the user is signed in previously or not, if not then it would prompt the user to sign in first. When registering, it would ask for which device it wants to use for authentication, the user can use the same current device in which he/she is browsing or they can select any other device to use to authenticate them. Then it would use FIDO2/WebAuthn to register users and save the users data in the MongoDB Database. If the user is already authenticated it would let the user to authenticate themselves and then access the dashboard. The dashboard shows the total number of passwords saved and the number of passwords needed to be updated.

Further it also allows users to "Create a Vault" where users can save passwords by adding website name, username and password and saving it. Additionally, it has the ability to determine how strong a password is and how long a supercomputer would need to break it. It also has the feature to generate a random password consisting of uppercase letters, lowercase letters, numbers, symbols which would be too hard to be cracked as shown in the section below.

It also has another section called "Vault" where users can see all the previously saved passwords.

Role of Authenticator (WebAuthn):-

1. The user tries to login to a website
2. The website prompts the user to authenticate
3. The user authenticates against their authenticator
4. Via the browser, the authenticator signs and returns a response to the website.
5. The website verifies the authenticator response.
6. The user is logged in.
7.

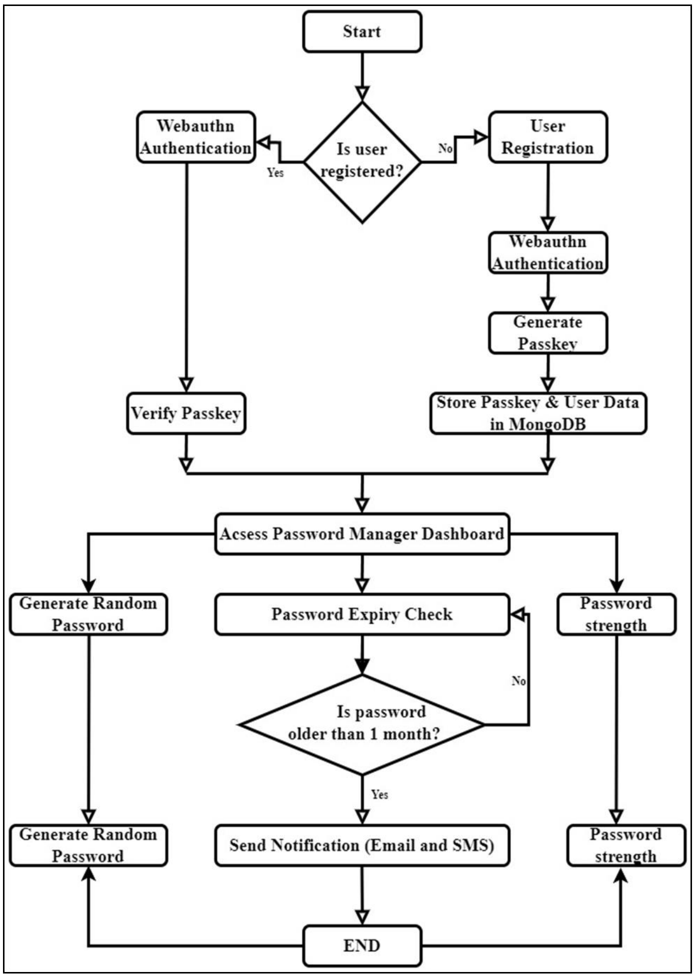


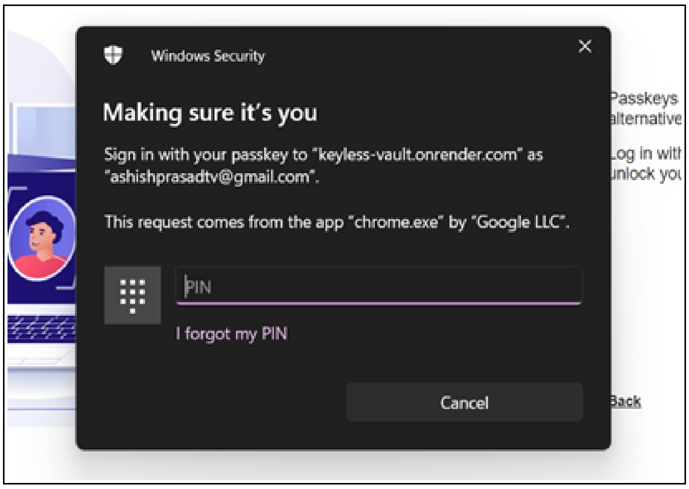
Figure 2: Flowchart of VaultGuard.
Source: Authors, (2024).

IV. RESULTS AND DISCUSSIONS.

The result set for the VaultGuard system includes various test cases that cover the primary functionalities and features of the platform. The registration and login process are a critical aspect of the platform, and it should be thoroughly tested to ensure that users can register and log in to the platform without any issues. This includes testing the password-less login using WebAuthn and verifying that the device is connected using valid credentials.

The normal functions of the VaultGuard, such as viewing, adding, editing, and deleting passwords, should also be tested to ensure that users can manage their passwords effectively. The system should allow users to generate a new random password and display the estimated time to crack this password, ensuring that users can create strong and secure passwords. The search functionality should be tested to ensure that users can search for a specific password quickly and efficiently.

The password aging notification feature should be tested to ensure that users receive notifications via email and SMS when their password is older than one month. This feature is essential for maintaining the security of user accounts and ensuring that users regularly update their passwords.


Windows Security

Making sure it's you

Sign in with your passkey to "keyless-vault.onrender.com" as "ashishprasadtv@gmail.com".

This request comes from the app "chrome.exe" by "Google LLC".

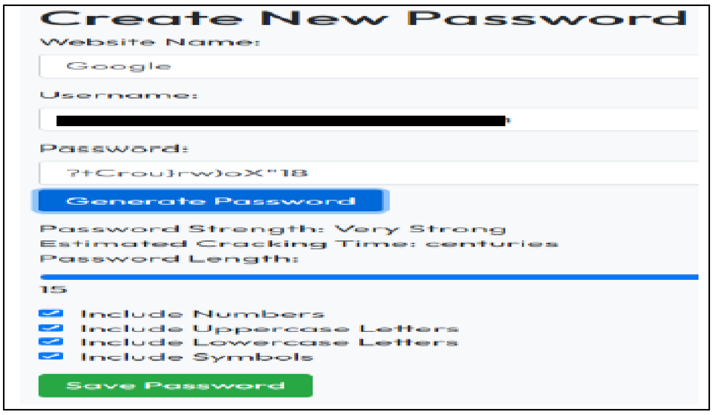
PIN

I forgot my PIN

Cancel

Figure 3: Same Device SignIn.
Source: Authors, (2024).

While logging into the device using the same device as shown in Fig. 3, it shows this prompt to let the user sign in or register itself using the system prompt popup to sign in using the system pin generated by the user during login.


Create New Password

Website Name:

Google

Username:

[redacted]

Password:

?+Crou}rw)oX"18

Generate Password

Password Strength: Very Strong
Estimated Cracking Time: centuries
Password Length:

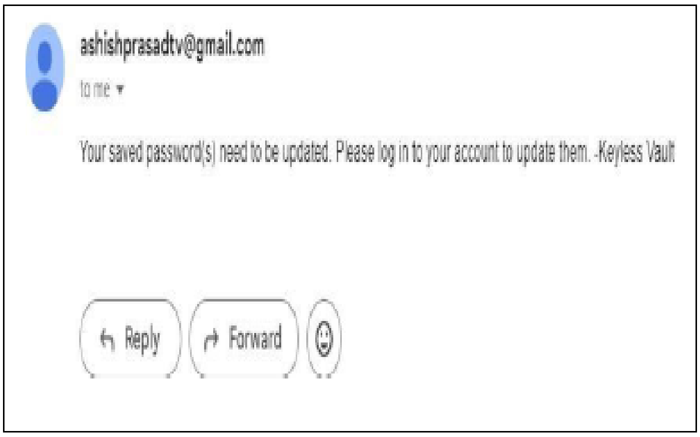
15

☑ Include Numbers
☑ Include Uppercase Letters
☑ Include Lowercase Letters
☑ Include Symbols

Save Password

Figure 4: Create Vault.
Source: Authors, (2024).

As a result, the system allows the user to save the password in the vault and to generate a new random password with letters including uppercase, lowercase, numbers and symbols as shown in Fig. 4. It also shows the strength of the password and Estimated Cracking Time by Brute Force Algorithm.



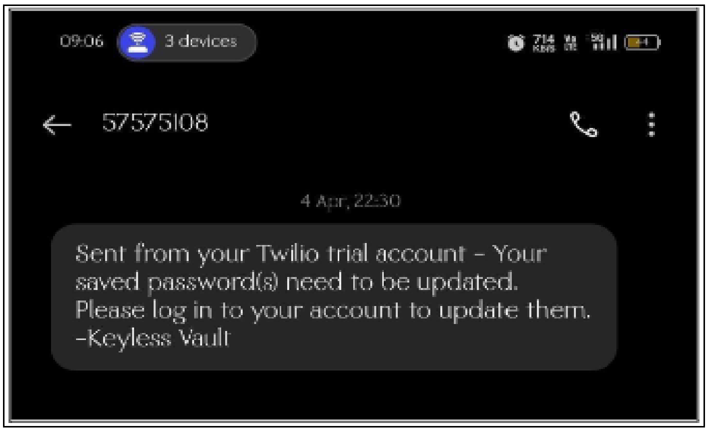
ashishprasadtv@gmail.com

to me ▾

Your saved password(s) need to be updated. Please log in to your account to update them. -Keyless Vault

Figure 5: Email Notification.
Source: Authors, (2024).

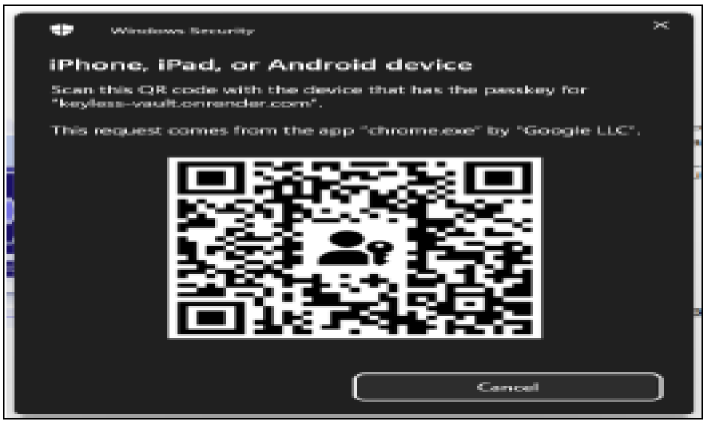
When the password is older than 1 month the server will send a mail to the user that the password needs to be updated as shown in Fig. 5.



Sent from your Twilio trial account - Your saved password(s) need to be updated. Please log in to your account to update them. -Keyless Vault

Figure 6: SMS Notification.
Source: Authors, (2024).

Fig. 6 displays that the server also sends an SMS Notification to the registered users' mobile number reminding him/her to update its password as it is older than 1 month.



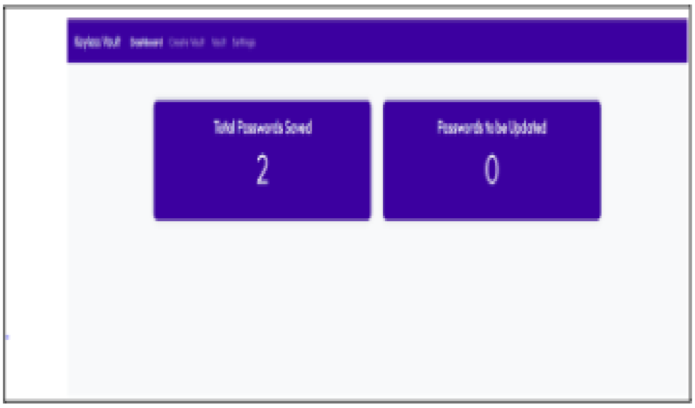
iPhone, iPad, or Android device

Scan this QR code with the device that has the passkey for "keyless-vault.onrender.com".

This request comes from the app "chrome.exe" by "Google LLC".

Figure 7: Using different device to Sign In.
Source: Authors, (2024).

While logging into the device using any other device, it shows a QR code, which the user has to scan using its smartphone which when scanned will prompt the user to sign in using his/her device and save the pass keys in that device and allow them to use the same device in future to sign in to the dashboard as shown in Fig. 7.



Total Passwords Saved
2

Passwords to be Updated
0

Figure 8: VaultGuard Dashboard.
Source: Authors, (2024).

Figure. 8 shows the dashboard consisting of the total number of passwords saved and the number of passwords needed to be updated.

Table 2: Comparative Analysis.

Sr No.	Research paper Title	Proposed Methodology	Drawbacks
1	VaultGuard: The Advanced Keyless Security System	FIDO2/WebAuthn	may not integrate well with specific third-party applications
2	Building and Studying a Password Store that Perfectly Hides Passwords from Itself [1]	SPHINX	work on non-confidential channel, limited adoption
3	Resilient Password Manager Using Physical Unclonable Functions [2]	PUF	Such a scheme cannot operate without a backup in case of catastrophic failure of the PUFs. Extra Hardware level security
4	A Password- Based Authentication Based on the CAPTCHA AI Problem.[3]	CAPTCHA AI	Limited Accessibility, Adversarial Attacks, False Positives
5	Securing password using dynamic password policy generator algorithm [4]	Dynamic Password Generator	Memory Load, Training and Education, Increased Support Requests

Source: Authors, (2024).

Overall, the test cases for the VaultGuard system should ensure that the platform is secure, user-friendly, and functional. The testing covers all the primary functionalities and features of the platform, including registration, login, password management, random password generation, and password aging notification. The testing should also ensure that the platform is compliant with relevant security standards and regulations.

V. PERFORMANCE METRICS

Understanding the critical elements that affect an accuracy of a Keyless Vault (a password manager based on FIDO2/WebAuthn) is necessary to determine its accuracy. Accuracy here refers to the system's capacity to appropriately approve authorized users and deny illegal ones.

Definitions:

True Positive Ratio (TPr): Legitimate users who are correctly authenticated.

False Positive Ratio (FPr): Unauthorized users who are incorrectly authenticated.
True Negative Ratio (TNr): Unauthorized users who are correctly rejected.
False Negative Ratio (FNr): Legitimate users who are incorrectly rejected.
The research work has been tested for 150 legitimate authentication attempts and 150 unauthorized authentication attempts. Out of the 150 legitimate users, 145 are correctly authenticated (TPr), and 05 are incorrectly rejected (FNr). Out of the 150 unauthorized users, 148 are correctly rejected (TNr), and 02 are incorrectly authenticated (FPr).

Accuracy Metrics:

1. Accuracy: Accuracy gives the overall correctness of the system, combining both authentication successes and failures.

$$\text{Accuracy} = (TPr + TNr) / (TPr + TNr + FNr + FPr) \quad (1)$$
$$\text{Accuracy} = (145+148) / (145+148+02+05) = 293 / 300$$
$$\text{Accuracy} = 0.9766 = 97.66\ \%$$

2. Precision (for accepted users): Precision represents how well the system avoids false positives, i.e., how many of the users it accepts are actually legitimate.

$$\text{Precision} = TPr / (TPr + FPr) \quad (2)$$
$$\text{Precision} = 145/(145+02) = 0.9863 = 98.63\%$$

3. Recall (also known as True Positive Rate or Sensitivity): Recall indicates how many legitimate users are correctly authenticated.

$$\text{Recall} = TPr / (TPr + FNr) \quad (3)$$
$$\text{Recall} = 145/(145+05) = 0.9666 = 96.66\%$$

4. False Positive Rate (FPR): FPR shows the likelihood that an unauthorized user gets authenticated.

$$\text{False Positive Rate} = FPr / (FPr + TNr) \quad (4)$$
$$\text{False Positive Rate (FPR)} = 02/(02+148) = 0.0133$$
$$\%\text{False Positive Rate } (\%FPR) = 1.33\%$$

5. False Negative Rate (FNR): FNR is the likelihood that an authenticated user will have their authentication refused.

$$\text{False Negative Rate} = FNr / (TPr + FNr) \quad (5)$$
$$\text{False Negative Rate (FNR)} = 05/(145+05) = 0.0333$$
$$\%\text{False Negative Rate } (\%FNR) = 3.33\%$$

Table 3: Feature Analysis.

Paper	Algorithm used	Encryption Technique	SMS Notification	Mail Notification
[1]	secure multiparty computation (MPC)	homomorphic encryption	NO	NO
[2]	PUF-based key generation	AES	NO	NO
[3]	dynamic password policy generator	SHA or PBKDF2	NO	NO
[4]	CAPTCHA AI	SHA-256	NO	NO
Proposed System	FIDO2/WebAuthn	AES 256	YES	YES

Source: Authors, (2024).

The proposed system VaultGuard sets a new standard for secure and user-friendly password management systems, effectively addressing the shortcomings of traditional methods with 97.66 % accuracy, 98.63% precision recall value as 96.66%, FPR & FNR as 1.33 % and 3.33% respectively.

VI. CONCLUSION

The “VaultGuard” represents a significant advancement in password management and authentication technology. Through its integration of FIDO2/WebAuthn for password-less authentication and AES 256-bit encryption for secure password storage, this system addresses the major vulnerabilities inherent in traditional password-based systems. The implementation of these technologies not only enhances security but also improves the user experience by simplifying the authentication process and reducing the cognitive load on users.

Moreover, the addition of an automated password generator and a proactive password aging and notification system further strengthens the system's security posture by ensuring that passwords are both strong and regularly updated. The user-friendly interface, developed with NodeJS and EJS, ensures that the system is accessible to a broad range of users, thus promoting better security practices across diverse user groups.

“VaultGuard” also benefits from the scalability and performance capabilities of MongoDB, making it suitable for deployment in environments ranging from small businesses to large enterprises. The system's focus on compliance and regular security audits guarantees that it remains effective against evolving cybersecurity threats[14][16].

In conclusion, “VaultGuard” is not just a tool for securing passwords but a comprehensive platform for promoting a more secure digital environment. Its innovative approach to password management could potentially set a new standard for how personal and organizational security is managed in an increasingly interconnected world.

.

VII. AUTHOR’S CONTRIBUTION

Conceptualization: Dr. Yogita Mane, Dr. Neeta Patil and Akshay Agrawal
Methodology: Dr. Yogita Mane, Sanketi Raut and Vishal Shinde.
Investigation: Dr. Yogita Mane, Akshay Agrawal.
Discussion of results: Dr. Yogita Mane, Dr. Neeta Patil, Akshay Agrawal, Sanketi Raut and Vishal Shinde.
Writing – Original Draft: Dr. Yogita Mane. Akshay Agrawal.
Writing – Review and Editing: Sanketi Raut and Dr. Neeta Patil.
Resources: Vishal Shinde and Akshay Agrawal.
Supervision: Dr. Yogita Mane, Dr. Neeta Patil and Vishal Shinde.
Approval of the final text: Dr. Yogita Mane, Dr. Neeta Patil, Akshay Agrawal, Sanketi Raut and Vishal Shinde.

VIII. REFERENCES

[1] M. Shrivanian, N. Saxena, and S. Jarecki, “Building and Studying a Password Store that Perfectly Hides Passwords from Itself,” in Proc. IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017.

[2] M. Mohammadi Nodoushan, B. Cambou, and C. R. Philabaun, “Resilient Password Manager Using Physical Unclonable Functions,” in Proc. IEEE 41st International Conference on Distributed Computing Systems (ICDCS), 2021.

[3] M. Alajmi, I. Elasshry, and H. S. El-sayed, “A Password-Based Authentication System Based on the CAPTCHA AI Problem,” in Proc. IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017.

[4] A. Singh and S. Raj, “Securing password using dynamic password policy generator algorithm,” August 8, 2021.

[5] J. Bonneau, “The science of guessing: Analyzing an anonymized corpus of 70 million passwords,” in Proc. IEEE Symp. Secur. Privacy, 2012, pp. 538–552.

[6] I. Dacosta, M. Ahamad, and P. Traynor, “Trust no one else: Detecting MITM attacks against SSL/TLS without third-parties,” in Proc. Eur. Symp. Res. Comput. Secur., 2012, pp. 199–216.

[7] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in Proc. IEEE Symp. Secur. Privacy, 2012, pp. 553–567.

[8] M. Gusev, S. Ristov, G. Velkoski, and P. Gushev, “Alert Notification as a Service,” in Proc. 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).

[9] D. J. Bernstein, M. Hamburg, A. Krasnova, and T. Lange, “Elligator: Elliptic-curve points indistinguishable from uniform random strings,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2013, pp. 967–980.

[10] S. S. Madugula, “Improvement of Passkey Entry Protocol for Secure Simple Pairing,” in Proc. 2023 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC).

[11] S. Chiasson, P. C. van Oorschot, and R. Biddle, “A usability study and critique of two password managers,” in Proc. 15th Conf. USENIX Secur. Symp. - Vol. 15, 2006, Art. no. 1.

[12] S. Kumar, S. Huzaimah, Y. Binti, and A. Hamid, “Real time mailbox alert System via SMS or Email,” in Proc. 2007 Asia-Pacific Conference on Applied Electromagnetics.

[13] R. Chatterjee, J. Bonneau, A. Juels, and T. Ristenpart, “Cracking resistant password vaults using natural language encoders,” in Proc. IEEE Symp. Secur. Privacy, 2015, pp. 481–498.

[14] W. Ford and B. S. Kaliski Jr , “Server-assisted generation of a strong secret from a password,” in Proc. 9th IEEE Int. Workshops Enabling Technol.: Infrastructure Collaborative Enterprises, 2000, pp. 176–180.

[15] M. J. Freedman, Y. Ishai, B. Pinkas, and O. Reingold, “Keyword search and oblivious pseudorandom functions,” in Proc. 2nd Int. Conf. Theory Cryptography. 2005, pp. 303–324.

[16] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov, “The most dangerous code in the world: Validating SSL certificates in non-browser software,” in Proc. ACM Conf. Comput. Commun. Secur., 2012, pp. 303–324.