IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13487

Cipher Safe: Your Digital Password Guardian

Mrs. Harshitha S[1], Siri H L[2], Srushti K[3], Tarang Madduri[4], Vidwath K T[5]

Assistant Professor, Department of Computer science and Engineering, Malnad College of Engineering[1]

UG Student, Department of Computer science and Engineering, Malnad College of Engineering[2-5]

Abstract: An innovative approach called "Cipher Safe: We intend to unveil on the market the "Digital Password Guardian" product which was created to make strong the password protection of internet services. It is a highly efficient method, a much-needed measure in our data insecurity system. It offers the simplest, yet the most effective way of dealing with preventing password compromise and any further unwanted access. Cipher Safe is as it can be a total mender of the current security woes that are caused by shortcomings such as interruption of the operation and delay in identification through biometric authentication as well as key exchanging that are on the updated mode. Participation in the program empowers people to train and have a clear understanding of the key password practices which is beneficial in that they can guard their identities more safely by having online portfolios too. By being the leaders in the technology averse to the threats, we are always at the tricky part of safeguarding ourselves against such vulnerabilities that are common thing in the bitcoin industry. This is because we continue updating and upgrading our software as soon as the threats are detected. The term does not provide any private user information, even if it complies with the best practices security protocols by employing encryption mechanisms which is presented with strong encryption; therefore, it could save any information regarding the user. It does not matter what platform users are utilizing - all the technologies are symmetric thanks to the Cipher Safe that ensures interoperability, and thereby cybersecurity. With Cipher Safe, over and above the function of a typical password manager, you will experience enhanced safe session gentrification and a broader scope of overall security.

Keywords: Cipher Safe, Encryption

I. INTRODUCTION

Presenting "Cipher Safe: A digital password protection slogan, also known as "Digital Password Guardian," which could change the way we think about password protection in the modern world. It is becoming increasingly apparent that adequate protection systems are a greater necessity than ever because there is a breakthrough in cyber attacks and data breaches, which is commonplace. Cipher Safe is a specially-made company that is always first in line with innovations, and the user is allowed to keep their private data highly secure. The present-day cryptographic algorithms lie in the heart of Cipher Safe operations and make provision for the most security it is possible to give to the digital profiles and passwords of our users. With the Cipher Safe, the user can create and store difficult, one-time passwords without much hassle too.

Cipher Safe makes it easier for users who are dealing with passwords, by introducing a user-friendly interface, users can save their credentials on several platforms and devices and have them securely retrievable. Cipher Safe counter-strengthens these protective actions that pop up by employing the most sophisticated schemes like biometric identification and multi-factor authentication. All such attempts by unauthorized individuals are thus thwarted.

Cipher Safe always has taken the protection and security of user privacy and data as their top priorities by applying very close security keeping away from unauthorized access and data leakage. Cipher Safe is being constantly upgraded and updated not only to improve the ability to counteract new perils with time and the wishes of users but also, of course, due to the growth of technology. In the process, combined with knowledge and awareness spread regarding password security steps, Cipher Save brings people about their online privacy ownership.

It becomes clear that Cipher Safe's core lies in its effortless integration and non-platform dependence, and for both individuals and companies that are aiming at possessing sharp defence strategies of online protection, Cipher Safe is the right solution. Computing nowadays revolves around passwords and users. On the occasion of the firm's product launch, the founder is thrilled to invite you, our faithful Cipher Safe trans, to join us in safeguarding all your digital assets and creating a robust future.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13487

II. RELATED WORK

“Password Managers” by author Neil J. Rubenking on May 21, 2021, Myriad teachings have of late shown the Keeper to be a secure and practical password manager. Consider for instance in a 2019 study conducted by experts at the University of California, Berkeley that Keeper is one of the best password managers because it hasn’t had security flaws detected. (2).

“Password Managers: It's All About Trust and Transparency” by Fahad Alodhyani on October 30, 2020. Several studies showed that Keeper is a legitimate tool for easier password management. For example, UM researchers observed that Keeper users were more likely to utilize strong passwords and less likely to reuse them on multiple sites in a 2018 investigation whereas other password managers' users faced such problems. (3).

"Perfect Passwords: Edition, Protection, Authentication" is the title of the publishing from the writer Mark Burnett in the year 2019 .The book by Mark Burnett contains authorization, security and secret key selection procedures. Cipher Safe's solution to password management then can be built with his knowledge leading to a strong security approach. Burnett's book doesn't just concentrate on the techno-side of password security, but also on the human factor of the password creation and management. With a detailed knowledge of user behavior and standard password management problems, Cipher Safe may be generated including the features that will make password derivation easy and at the same time reduce the probability of there being loopholes for vulnerability. This multifaceted approach, synergizing technical knowledge with behavioral tips, strengthens the position of Cipher Safe as a more mighty and easy password keeper. (4).

“No More Painful Password Management With AI” by Robert Biddle and Elizabeth Stobert on September 15, 2014. Password problems are well-known: users' websites a solid passwords that are hard to remember, have too many passwords and experience difficulty connecting their various passwords with their accounts. Two examples of password security solutions that take into account the issues of convenience to remember and password retention are password managers and cued graphical passwords. Our way forward to overcome the current limitations of password memorability and password portability is Versipass, a password manager that combines the best out of password managers and cued graphical passwords. We deploy diagram kehittäjät, which provides graphical passwords rather than the passwords. This feature serves as a crutch for users to reflect on their passwords and the associated accounts. (5).

III. OBJECTIVE

As you have noted properly and scheduled it in safe and secure notes storing and management of Cipher Safe acting as digital password guardian could be carried out.
The following are a few of the goals of Cipher Safe:

- Offer a place to hide private notes: Cipher Safe is designed to prevent unauthorized access to your notepad by encryption these notes with the well-known and strong AES-256 algorithm. T truth is that it is a safe location to save your confidential information such as bank numbers, passwords and login details.

- Manage and organize notes effectively: In your case, you have the option to group your hidden Notes in separate folders using a customized naming that you like. Through this, the needed information is located precisely and at the right time. Furthermore, through the utilization of keyword searches or phrases, you may scan the notes to locate those notes that you are after.

- Synchronize notes between devices: Keeper Notes enables you to sync notes among its Windows, iOS, and Android apps so that you can read them on your mobile devices or PC. It ascertains the fact that whatever the device you may use you will always view your latest notes.

- Attach files to notes: You can get attachments such as PDFs, documents, supplemental text, music, texts, words and much more with these hidden notes. Instead of having to create a more detailed sheet or separate notebook, this way you can keep extra information or reference resources in this area as well as your notes.

- Safely share notes with others: The safe-Notes feature can be used to share notes openly with other learners. You may label the people whom you assign to modify, remove, and view only notes while the others cannot access them.

- Securely destroy notes: Be aware of discarded dates when you stop using secret notes in them. However, that will take the note out of the box that you sent and prevent its reclaiming.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.13487

- Supply clients with a tool that is easy and reliable for handling responsibility for passwords to other personal data.
- Familiarize with users on one-of-a-kind strong passwords for each website or app so they use a higher level of security for their data.
- It is recommended that users should spend less time on their password administrating tasks. The Final Point Of our discussion is that the Secret Notes app is a secure program that can be useful in the case of handling your sensitive data such as notes. It has strong end-to-end encryption which is compatible with its flexibility and is cross-platform. So, it becomes another powerful companion device for the secret password manager.

IV. PROPOSED WORK

The target of this method is to introduce the article's subject clearly and concisely.

The following process will be followed in the creation of the secret notes: The following process will be followed in the creation of the secret notes:

1. Requirements collecting: Accordingly, what users say about their needs will be the starting point. Focus groups, interviews, and surveys will be employed to this end. To personalize the product, focus groups, interviews, and surveys will be used.

2. Design: The group will turn to the development of its design after establishing more requirements. This would be done through database design, user interface bringing, and user experience (UX) implementation.

3. Development: The next task will be applied to the organizations to which the chosen design has been proposed. Among these tasks, writing code, reviewing the code, and fixing errors would be part of my role as a programmer.

4. Testing: The app is going to be put through thorough testing once the development is completed to ensure that this technology has achieved reliability and safety. Application testers (both humans and independent testers) will test the application.

5. Setting up: The application will take the path of the approvals and testing to go live whereby the users will be able to use it.

V. RESULT

Increased password security: With Keeper, passwords become secure and are encrypted in the vault which is saved in un-crackable storage.

- Less complexity in passwords: Keeper could be the ultimate password manager that will provide you a unique, strong PIN for every account – it will spare you from having to do that on your own.

- Lower chance of password reuse: Through Keeper’s automatic password generation function, a single password breach is much less likely to be a primary source for the hacking of many other accounts. This is because the user generates a different password for each account.

- Enhanced convenience: Keeper may so to speak spare you time and energy as the password is automatically saved the moment you log on to sites and apps.

App Signup:
Members who have registered must complete the information requested in the snapshot. "Create your Cipher Safe account" can be used to create the new account.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13487

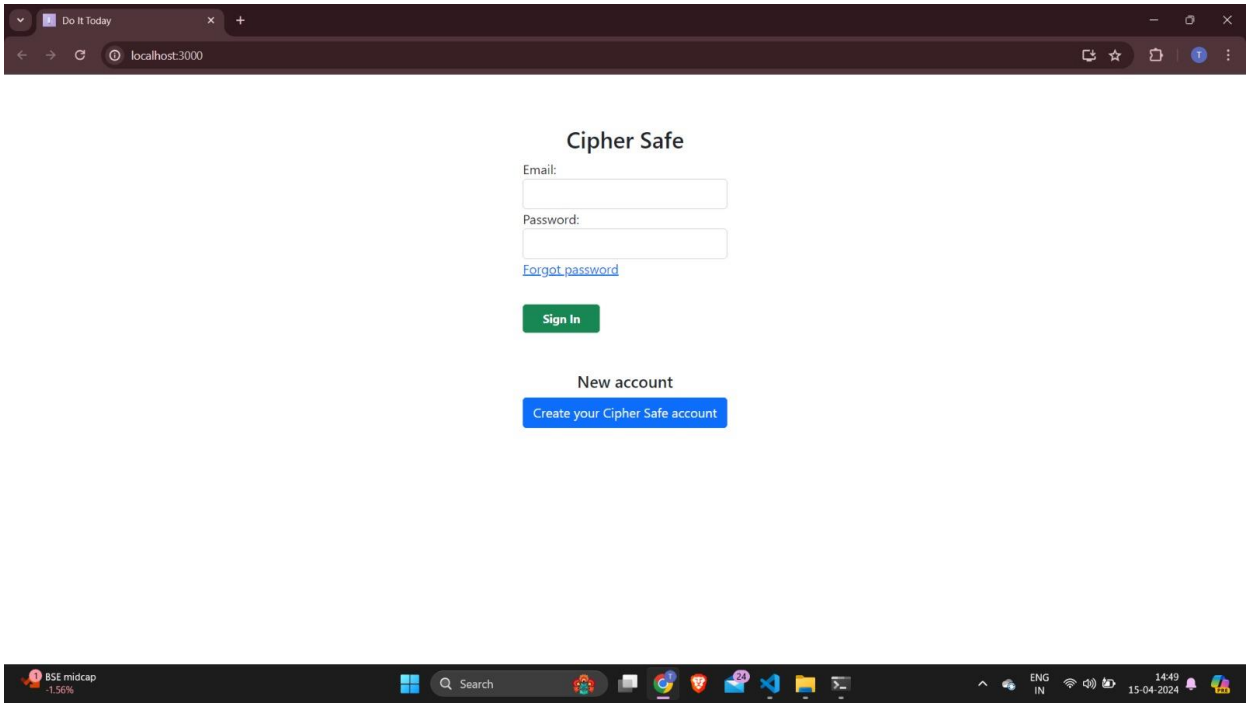

Fig. 1: Signup Page

App Login:
The picture and password storage details are provided in the snapshot below. The email will be saved as soon as we submit it with the password.

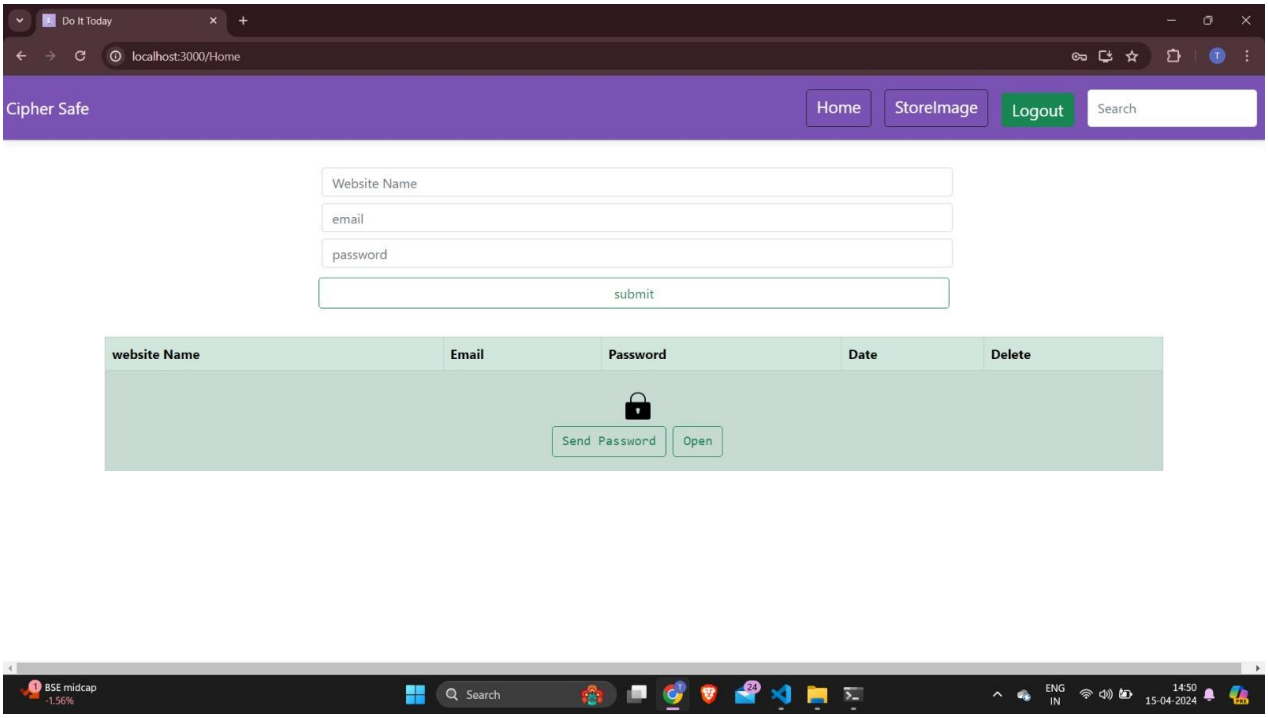

Fig. 2: Login Page

Password sent mail alert:
The transmit password button, which sends a passcode to the registered email address, must be used after submitting the passwords if we wish to review them again.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13487

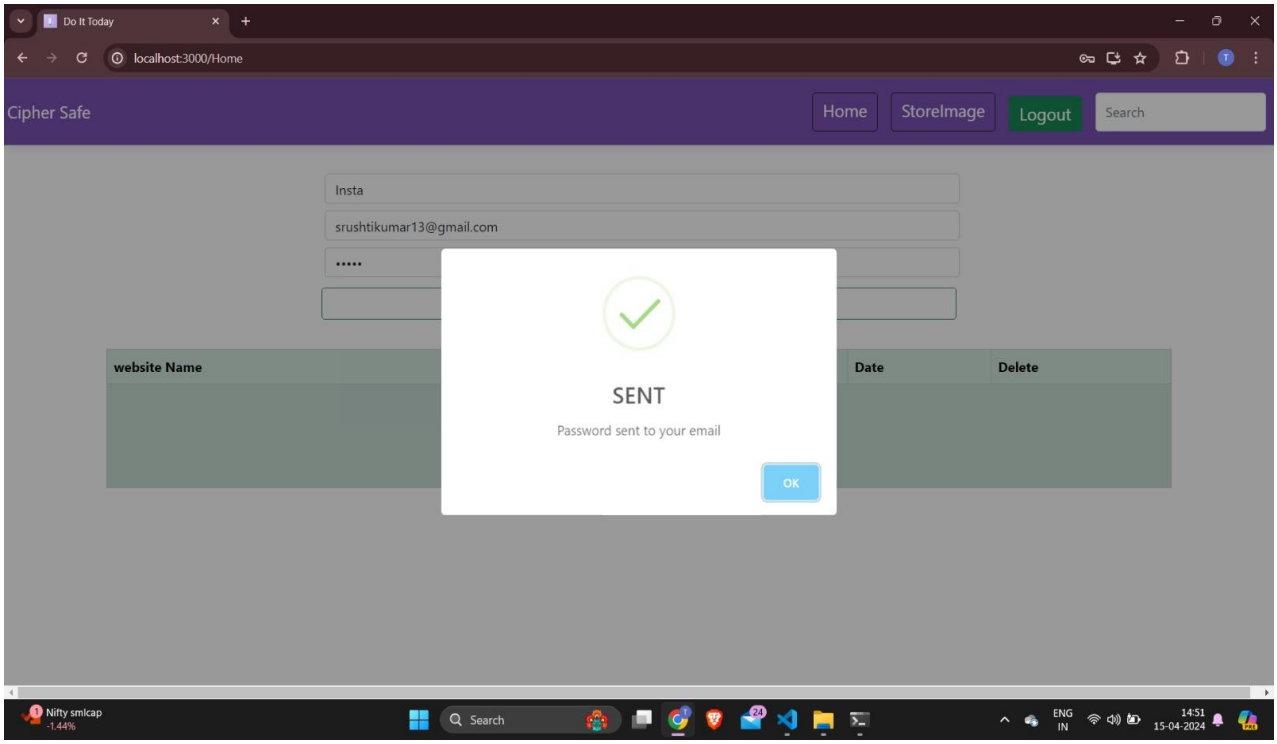

Fig. 3: Mail Alert

Password Alert:
As the registered person press the send password button, a pop-up message gets generated where we need to enter the passcode which is sent to our email.

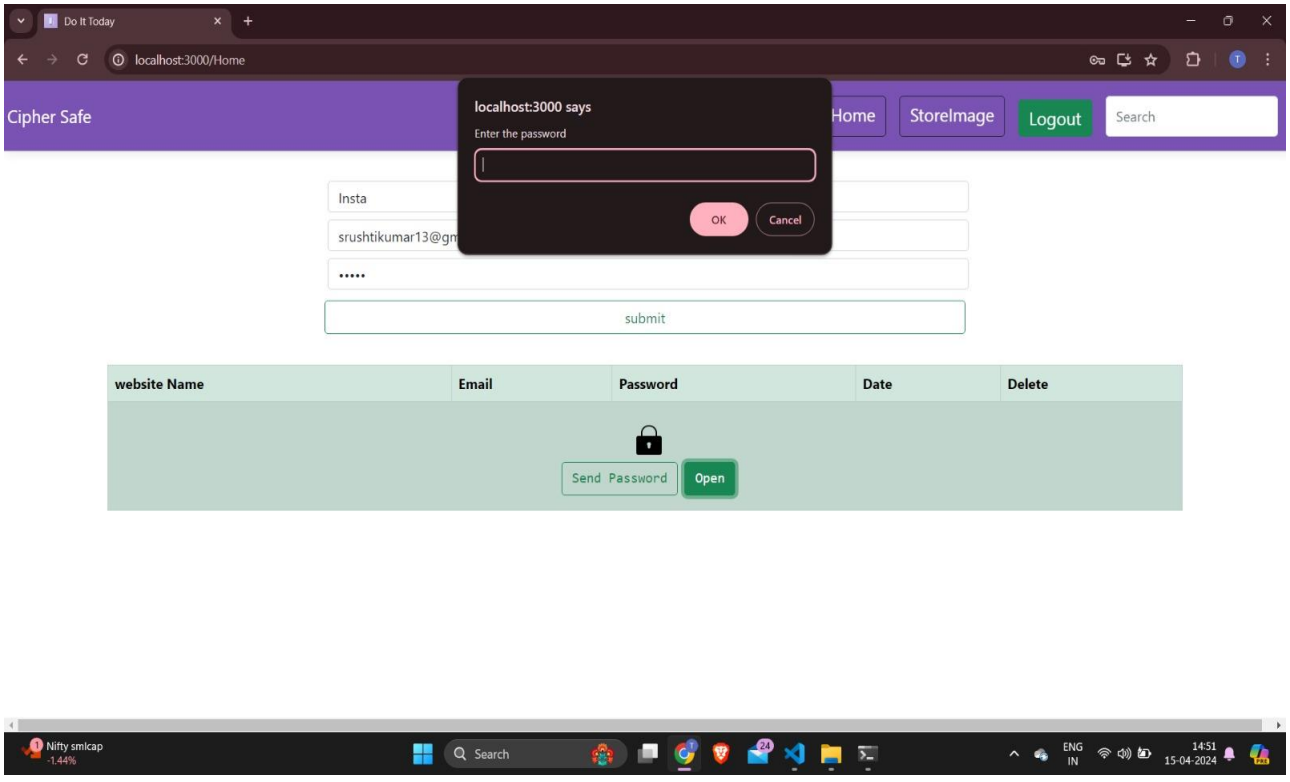

Fig. 4: Password Alert

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13487

Password Storage:
As we enter the passcode which is sent to our email, the hidden passwords will be visible. Further we can store any number of passwords.

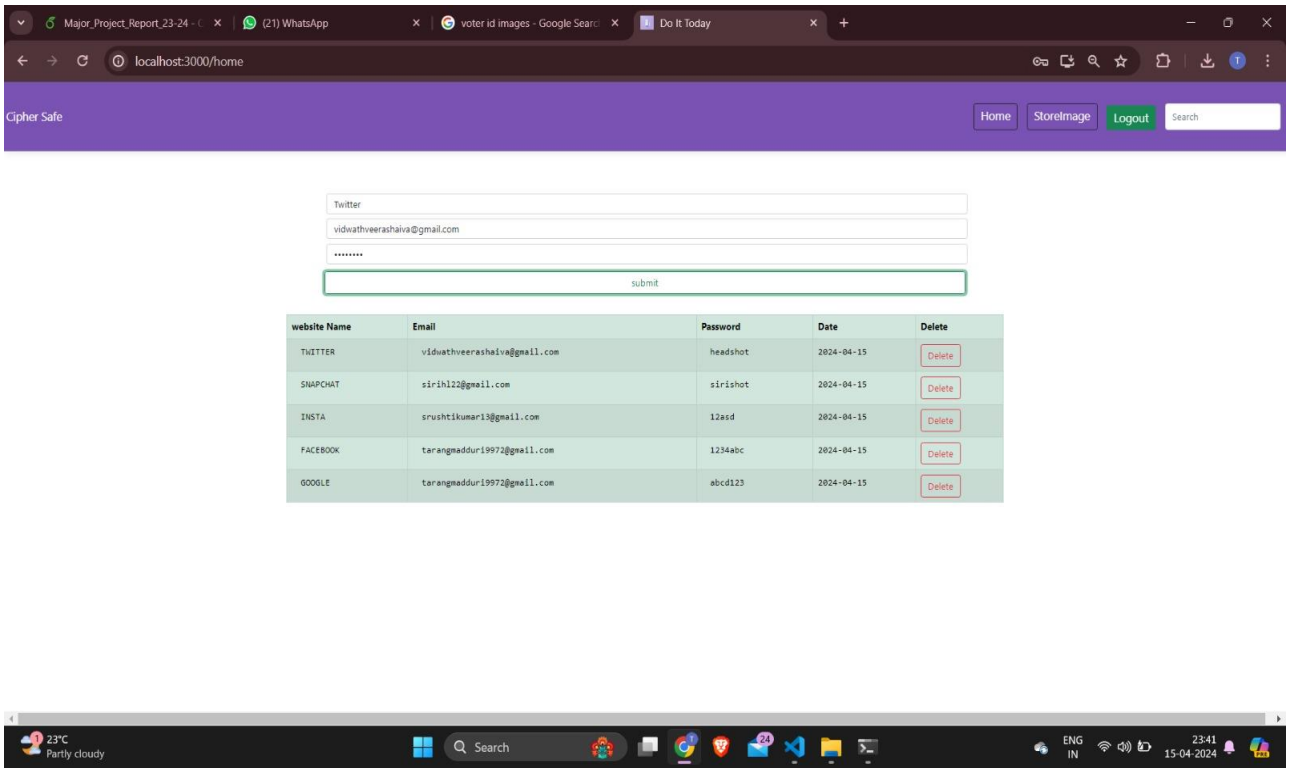

Fig. 5: Cipher Safe Storing Password

Image Storage:
In the taskbar there is a button named Store Image, where we can choose the files and can upload and store the image.

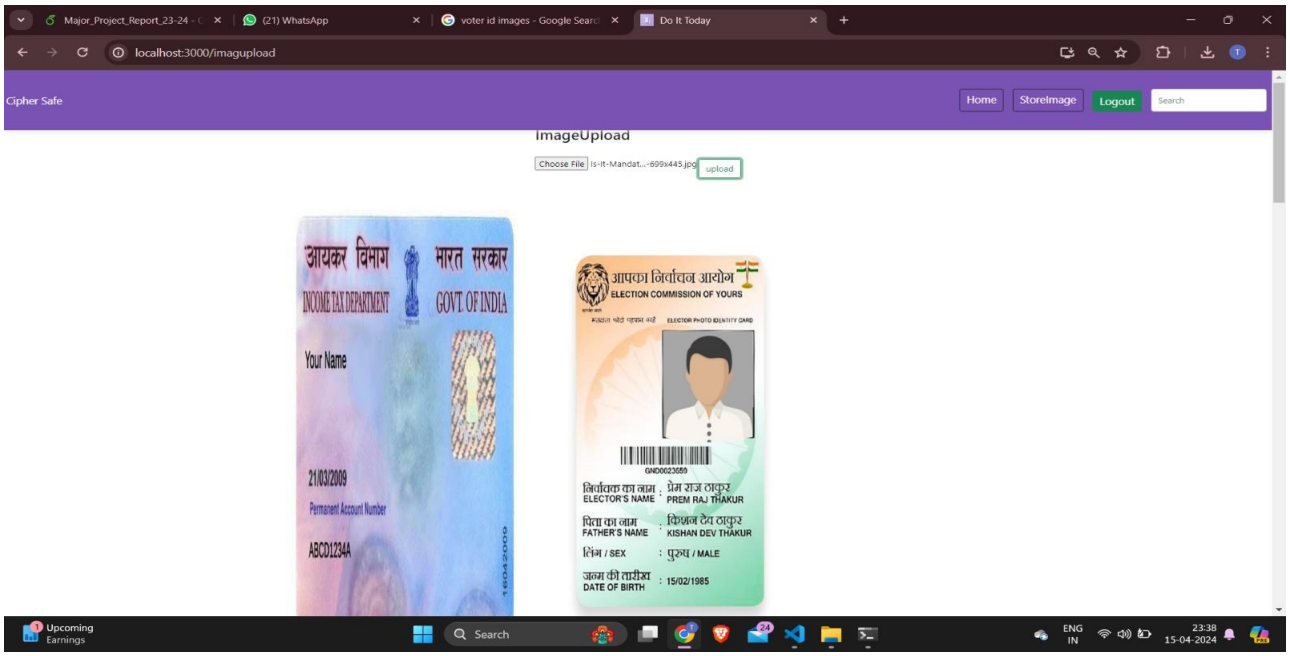

Fig. 6: Cipher Safe Storing Image

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024
DOI: 10.17148/IJARCCE.2024.13487

VI. CONCLUSION

With Cipher Safe's state-of-the-art encryption algorithms and singular authentication techniques, storing sensitive private data is made secure and simple. Besides that, the promotion of user education and their awareness conducive environment to preventive password hygiene and cybersecurity cultures is being applied. Cipher Safe takes as its mission, regularly, these updates and enhancements, which make its app fit any new sort of threats and everyday users' needs, helping it to remain in the first plan in the industry of password management technologies.

Cipher Safe is a true shining star in the murky data world that we all live in today as it empowers people by providing a clear and navigable pathway to online safety. Cipher Safe goes beyond other solutions that deal with password management and privacy by deeply concentrating on these factors while still integrating into their customers' digital environment. Cipher Safe may be regarded as a dependable partner that guarantees the security of the information more than the deteriorating physical barrier in the form of cyber attacks. Digital identity and passwords of users need to be reassured that they are safe as long as they have Cipher Safe overseeing the digital world from start to finish while they use it.

REFERENCES

[1]. Neil J. Rubenking, Password Managers - Title, Published - May 21, 2021.
[2]. Elizabeth Stobert, Robert Biddle, Password Manager that Doesn't Remember Passwords - Title, Published - 15 September 2014.
[3]. Fahad Alodhyani, Password Managers-It's All about Trust and Transparency - Title, Published – 30 October 2020.
[4]. R. Biddle, S. Chiasson, and P. C. van Oorschot. Graphical Passwords: Learning from the First Twelve Years. ACM Computing Surveys, 44(4), 2012.
[5]. J. Bonneau, M. Just, and G. Matthews. What's in a Name? In Financial Cryptography and Data Security, pages 98--113. Springer, 2010.
[6]. W. Cheswick. Rethinking Passwords. Queue, 10(12), Dec. 2012. S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B. Freitas Machado, A. Forget, N. Wright, G. Chan, and R. Biddle. The MVP Web-based Authentication Framework. In Financial Cryptography and Data Security, pages 1-8, Bonaire, Feb.2012.
[7]. S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle. Multiple password interference in text passwords and click-based graphical passwords. In CCS'09: Proceedings of the sixteenth ACM Conference on Computer and Communications Security, Chicago, USA, Nov. 2009. ACM.