

IncogSafe

Usable Security and Privacy (Course Project)

Team Name: Incog

Team Members: Anas Ahmad (2020023), Tanishqa Shital Singh (2020411)

PROJECT DETAILS

Our project is a password manager - **IncogSafe**, designed to store and manage passwords for various online accounts. The main objective of this project is to develop a password manager that securely stores user passwords and provides an easy way to access them when needed.

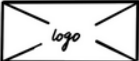
The password manager will have features such as password generation, password strength assessment, and storing other sensitive information such as personal details, OVD numbers (officially Valid Documents), and notes in encrypted form.


The application will use encryption algorithms to protect the passwords stored in the system, ensuring that only authorized users can access them. The user interface of the password manager will be designed to be user-friendly, with easy navigation and simple instructions.

Overall, the project aims to provide a secure and convenient solution for managing passwords, helping users

We conducted usability studies in many forms to get an idea of the user base, persona, features to be implemented, problem space, and how we can solve them. We used methods such as survey forms, literature review, competitor analysis and at last did a SWOT analysis on our interface.



LO-FI PROTOTYPE:





login id:

otp:

Welcome, user! 


Passwords


Notes


Details


logout


Manage Passwords


Socials 


website 1


website 2


website 3



Banking / Finance 

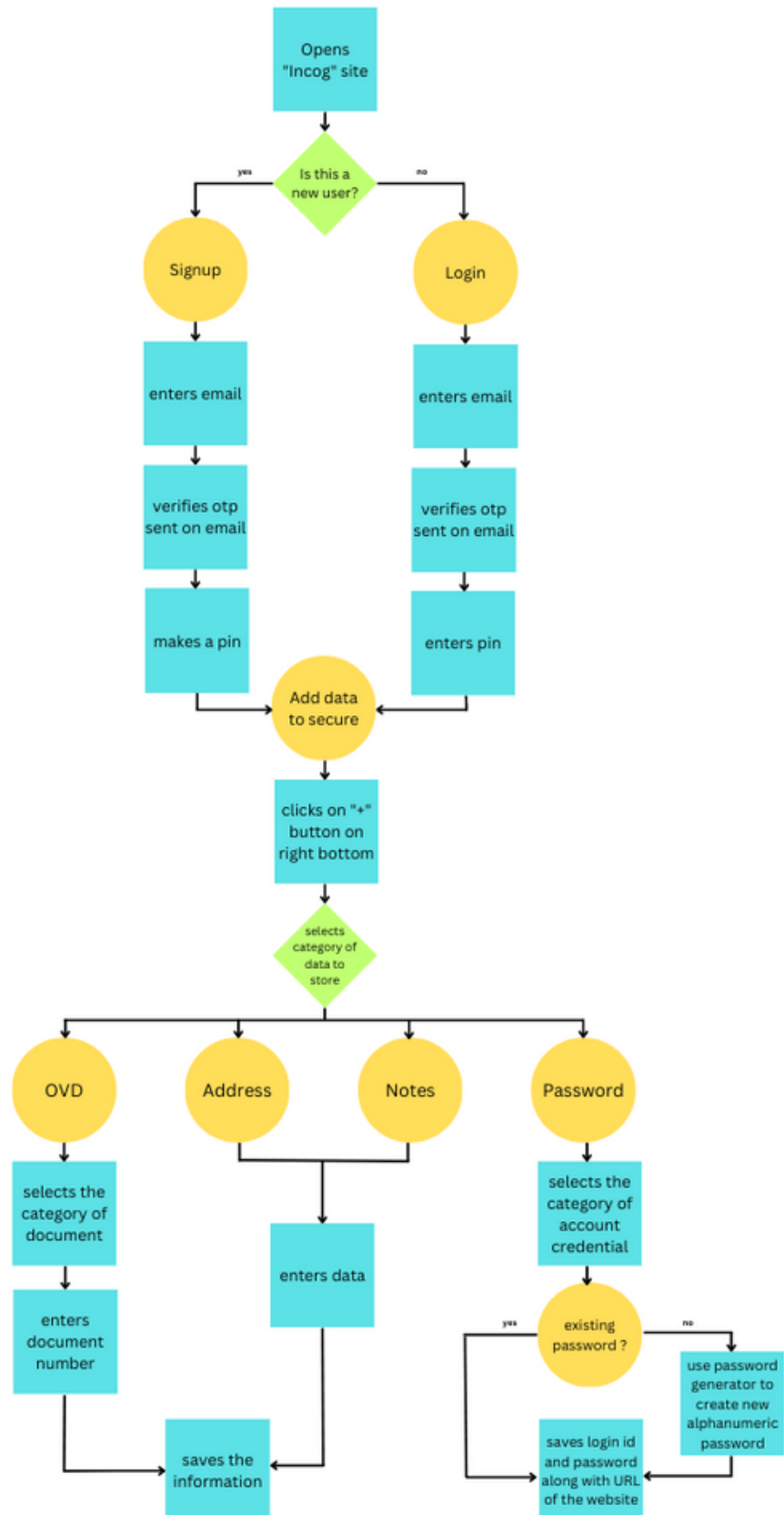
Wifi Routers 

Others 





WORKFLOW:

Link : <http://surl.li/falab>



RESEARCH STUDY METHODS:

Competitor's Analysis	 1Password	 Dashlane
Two-factor login	✓	✗
OVD number security	✓	✓
Notes security	✓	✓
Login type	Password + secret key	Password

From studying the competitors in the market, we concluded that most of the password managers on the market, along with saving password details, also give the features of storing OVD (officially valid document) numbers and notes with encryption to keep them safe. Dashlane didn't have two-factor authentication, which we aim to implement in our interface - IncogSafe.

Along with that, most password managers have alphanumeric text as password or a secret key. This ultimately requires a user to remember at least one master password somehow. In this case, if the master password security is somehow compromised it can lead to full security breach for a user in all his accounts.

Literature Review

Literature review of some studies related to password managers:

“Usability, security, and trust in password managers: A quest for user-centric properties and features” – This study compared the security and usability of different password managers. The outcome was that most Password managers were secure, according to the author. Still, many of the managers had usability problems that directly affected their usefulness.

Reference: <https://www.sciencedirect.com/science/article/abs/pii/S1574013718302533>

The Factors Influencing the Use of Password Managers by Hussain Alshahrani – This survey integrated the technology model with other factors on the use of password managers. Data was gathered using online questionnaires. There were 170+ participants from 6 different countries completing the questionnaire. The results show that ease of use, utility and user readiness positively affect attitude and are significantly related to the use of password managers.

Reference: <https://journals.nauss.edu.sa/index.php/JISCR/article/view/1939>

“It Basically Started Using Me:” An Observational Study of Password Manager Usage by Sean Oesch, Scott Routi, James Simmons, and Anuj Gautam –

Conducted observational interviews with 32 password managers. And Result was that many users simultaneously used the browser-based manager and a third-party manager. Which was perplexing usability and security issues. The survey emphasized the necessity of easy-to-enter and remember password technology.

Reference: <https://dl.acm.org/doi/10.1145/3491102.3517534>

These studies imply that password managers can increase password security and facilitate users' password management. Password managers need to be more effective, but there are still usability and user behavior issues that need to be resolved.

User Survey

Survey Link: <https://forms.gle/ZTFF7RSxacfAFmhh7>

Based on the findings in the competitor analysis and literature review, we conducted a user survey to ask our potential users what they think about already existing security solutions and if our ideas would help them manage their password security needs better.

RESULT OF USER STUDY:

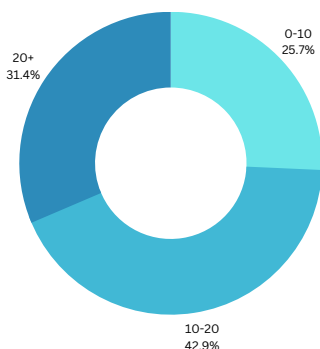
The results of the user survey was as follows :

As our study was mostly limited to our campus, most of the participants in our study were of age group 18-24 with 84% of them being students and rest being people with jobs in the technology sector.

The survey questionnaire was divided into 4 types of questions.

- Exploring how big the problem space is
- To identify existing problems that user face
- To get user perspective on features we aim to implement
- To get an idea on what creates best experience for a user

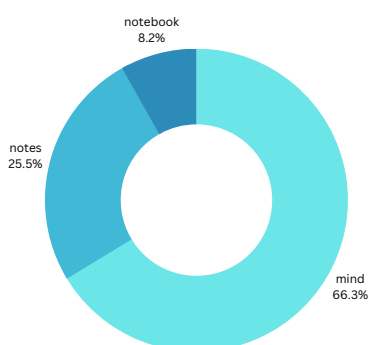
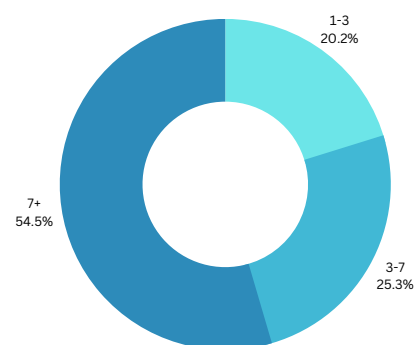
Section 1 : exploring problem space



Amount of online accounts requiring a password a user has.

In fact, a Dashlane analysis of data from more than 20,000 users in 2015 found that the average user has 90 online accounts.

Number of "different" password a user has for all online accounts



The way user keeps track of the passwords.

In Conclusion we found out that most of the user have more than 20 accounts online which require some sort of password protection.

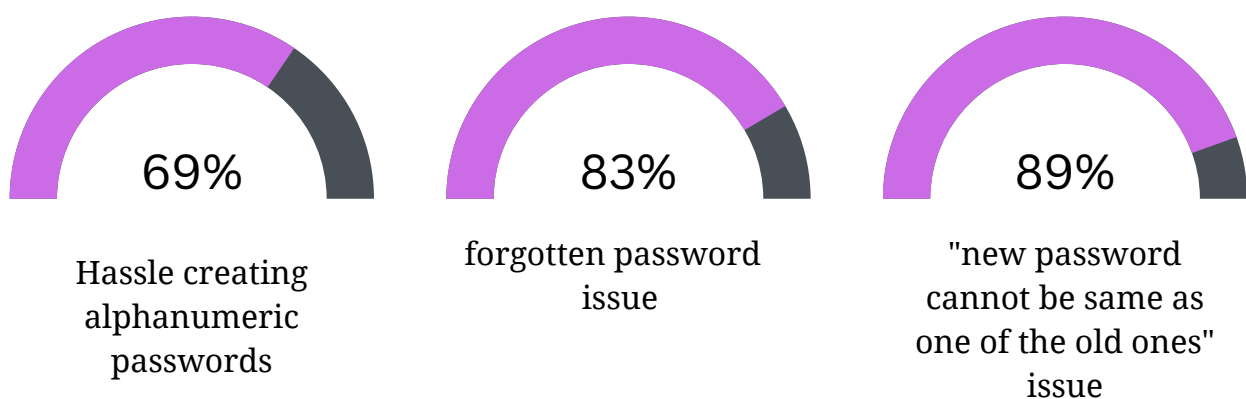
For these twenty accounts, users generally have only 5-7 passwords which might even be similar to each other.

Most of the users rely on their mind to remember these passwords.

This means that with such huge amount of online accounts, for utmost security we would need a many distinctive alphanumeric passwords that a user would try to memorise which is next to impossible.

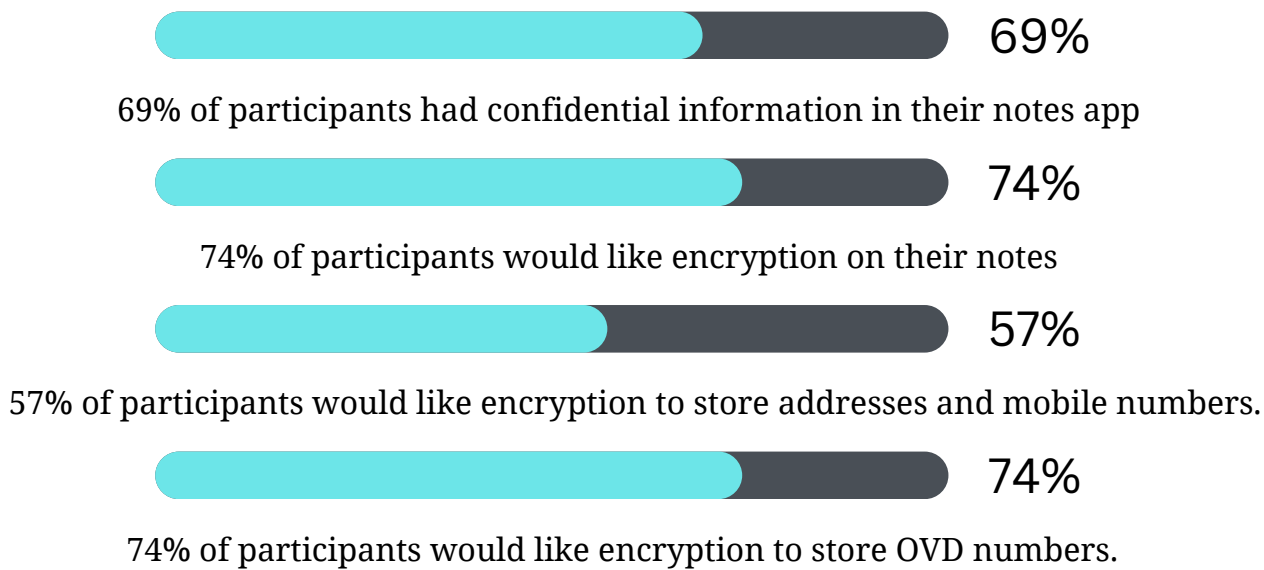
In both cases, a user creating distinct passwords or using same password, IncogSafe would act as a perfect solution as it can help user in storing it in encrypted database rather than to rely on his mind and also generate distinctive alphanumeric passwords for all of user's accounts.

Section 2 : identifying user problems



These problems were faced by a large percentage of the study participants. IncogSafe would help solve all three of them. Storing the passwords would help reduce forgotten password issues. The inbuilt alphanumeric text generator would help users to create new and distinct passwords that would not match the old ones as they would also be keepen track of.

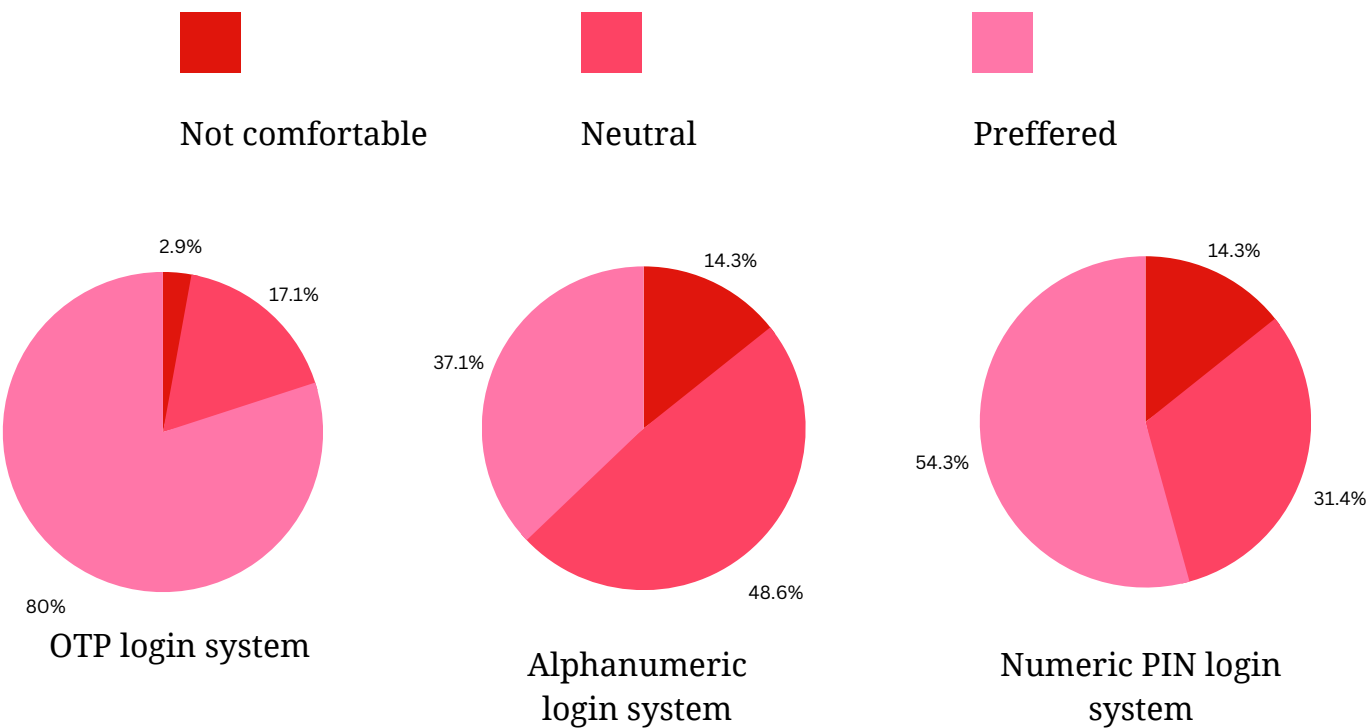
Section 3 : User perspective on features



These numbers show that major chunk of the participants of our study would use the features that we aim to offer in our interface - IncogSafe.

Section 4 : User experience

These questions was to get knowledge about what the users find most comfortable to login with so that we can make a easy user experience.



As seen from the above charts, Our platform IncogSafe would allow users to log in through the OTP verification system, which was the most preferable among the user participants.

In order to access specific passwords, the user would have to enter a numeric pin to re-verify their identity. This makes our platform two-factor authenticated.

We did not choose the alphanumeric password login method for our platform since most participants were neutral towards its usage due to the fact that it has been in use as a verification method on the internet for ages.

Since they preferred OTP and PIN to use, we opted for those verification methods.

SWOT analysis of IncogSafe

Link : <http://surl.li/faoca>

