

temenos

Instructions

1. This Hackathon consists of 2 rounds.
2. The 1st round will be a 24-hour coding round and the top 10-15 teams will be shortlisted for the 2nd round in which they have to present their solution.
3. Team size: 1-4 members.
4. Venue: CRC 101, 102, 103, 201
5. There are 4 problem statements, you can choose one of them.
6. Only offline submissions will be accepted.
7. All non-IITM participants should have a passport.
8. Problem statement will be released at 6 PM.
9. Registrations will be closed on 4th Jan at 6:30 PM.
10. Participants must be present at the venue till 10 PM, 4th Jan. (First four hours of the hackathon)
11. After that participants are allowed to leave, but they can stay back if they wish to stay at the venue.
12. Participants must be present at the venue from 3 PM to 6 PM on 5th Jan. (Last three hours of the hackathon).
13. If you face any queries, refer to the WhatsApp group. It's advised to be present at the venue so that we can resolve your queries quickly.
14. Onspot registrations are available.

Structure

Date & Time	Event
4th Jan 5:30 PM	Inauguration
4th Jan 6:00 PM	Kick off, PS release
5th Jan 5:30 PM	Round -1 ends
5th Jan 5:30 PM to 6:30 PM	Round -1 evaluation
5th Jan 7:00 PM	Top 10-15 Finalists Announcement
5th Jan 7:00 PM to 9:00 PM	Presentation by Finalists
5th Jan 9:00 PM	Winners announcement

docs.google.com

Personal
gettin started with Groww

IITK Hacks

IITM Hacks

Files to check

temp spam

Colorful Modern Business I...

My Application - Realtime...

Vishwa-docs/IIT-Madras-E...

+ New Tab

Encryptcon 24-Hr Hackath...

How to Enable USB debug...

Run apps on a hardware d...

Configure on-device devel...

Structure

Date & Time	Event
4th Jan 5:30 PM	Inauguration
4th Jan 6:00 PM	Kick off, PS release
5th Jan 5:30 PM	Round -1 ends
5th Jan 5:30 PM to 6:30 PM	Round -1 evaluation
5th Jan 7:00 PM	Top 10-15 Finalists Announcement
5th Jan 7:00 PM to 9:00 PM	Presentation by Finalists
5th Jan 9:00 PM	Winners announcement
7th Jan	Prize Distribution during the Encryptcon closing ceremony



temenos

Brief overview on banking services

Note: This is just a brief overview, participants are advised to go through online resources to get a clear idea about banking services.

Banking Services Overview:

Brief overview on banking services

Note: This is just a brief overview, participants are advised to go through online resources to get a clear idea about banking services.

Banking Services Overview:

1. Account Management:

Banking services include managing various types of accounts like savings, checking, loans, etc.

2. Transaction Processing:

Facilitating transactions including deposits, withdrawals, transfers, and payments.

3. Customer Authentication:

Verifying customer identity during logins, transactions, and other interactions.

4. Data Security:

Safeguarding sensitive information like personal details, financial records, and transaction history.

5. Regulatory Compliance:

Adhering to legal and industry standards to ensure data protection and privacy (e.g., GDPR, PCI DSS, etc.).

6. Risk Management:

Identifying and mitigating potential risks, such as fraud and cyber threats.

7. Credit card/Debit card etc.

Common Security Challenges:

1. Identity Theft:

Unauthorized access to personal information leading to fraudulent activities.

2. Phishing Attacks:

Deceptive attempts to acquire sensitive information like passwords or account numbers.

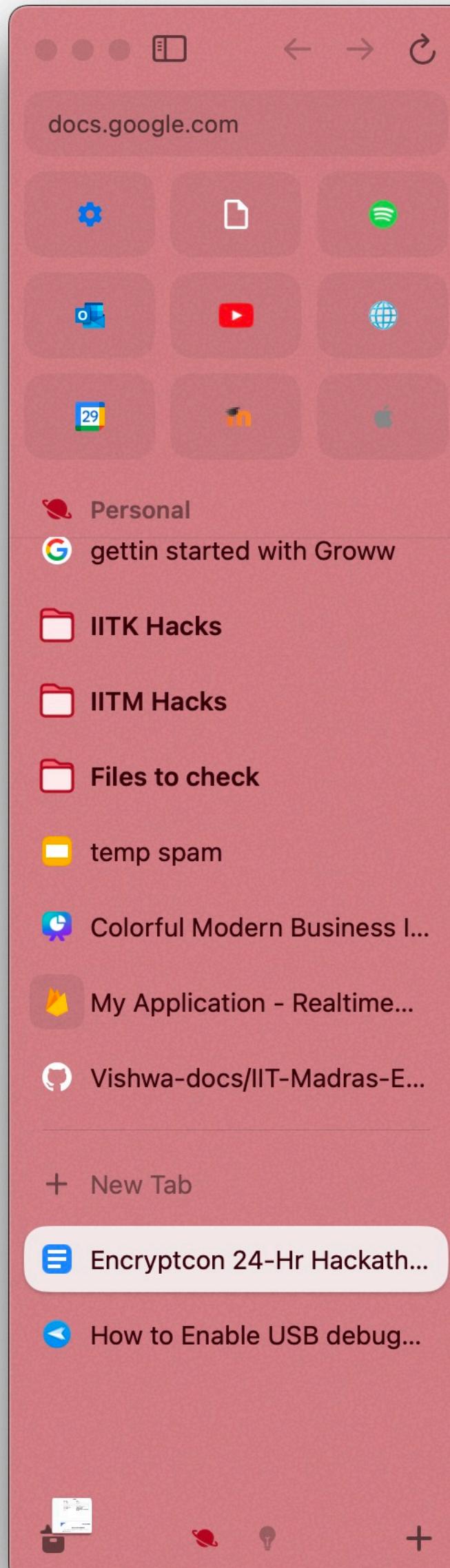
3. Weak Authentication:

Insufficient measures leading to compromised accounts or data breaches.

4. Data Breaches:

Unauthorized access to confidential data, compromising customer trust.

Functionalities that are currently in place:



docs.google.com

Personal

gettin started with Groww

IITK Hacks

IITM Hacks

Files to check

temp spam

Colorful Modern Business I...

My Application - Realtime...

Vishwa-docs/IIT-Madras-E...

+ New Tab

Encryptcon 24-Hr Hackath...

How to Enable USB debug...

Functionalities that are currently in place:

- **Multi-factor Authentication (MFA):**
Incorporating multiple layers of authentication (biometrics, OTPs, etc.) for enhanced security.
- **Identity Verification:**
Secure and efficient methods to verify user identity during login and transactions.
- **Encryption:**
Protecting sensitive data through robust encryption techniques.



temenos

Problem Statements

1. **Digital Identity Solutions for Secure and Sustainable Banking**
Track: "Digital Identity Assurance"
Challenge: Develop a self-sovereign digital identity solution that empowers customers to have more control over their personal data and identity verification processes within the banking ecosystem.

Considerations: (some ideas that can be used by participants)
Creating a decentralized identity system using blockchain or similar technology.
Allowing users to selectively share personal information with different banking services or entities.
Ensuring compliance with regulations while enabling user-controlled identity verification.
For Instance:
Conventional IAM solutions, particularly those dependent on usernames/passwords, are vulnerable to hacking, phishing, and various identity theft techniques. Commonly employed remedies include MFA and biometrics for login and transaction security to mitigate certain breaches. In addition to these measures, are there contemporary techniques we can explore, such as leveraging self-sovereign identity, to enhance security further?

Problem Statements

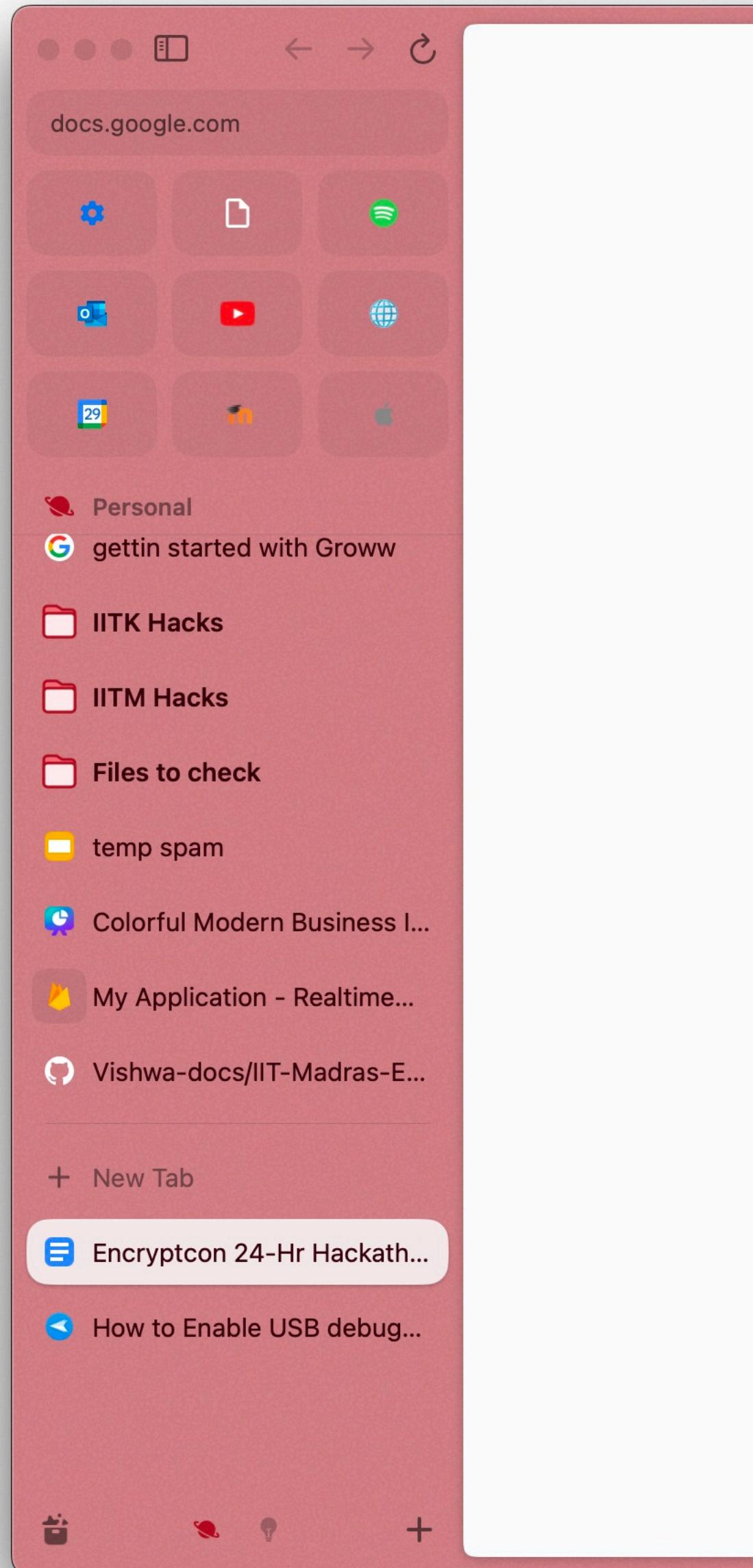
- 1. Digital Identity Solutions for Secure and Sustainable Banking**
Track: "Digital Identity Assurance"
Challenge: Develop a self-sovereign digital identity solution that empowers customers to have more control over their personal data and identity verification processes within the banking ecosystem.

Considerations: (some ideas that can be used by participants)
Creating a decentralized identity system using blockchain or similar technology.
Allowing users to selectively share personal information with different banking services or entities.
Ensuring compliance with regulations while enabling user-controlled identity verification.
For Instance:
Conventional IAM solutions, particularly those dependent on usernames/passwords, are vulnerable to hacking, phishing, and various identity theft techniques. Commonly employed remedies include MFA and biometrics for login and transaction security to mitigate certain breaches. In addition to these measures, are there contemporary techniques we can explore, such as leveraging self-sovereign identity, to enhance security further?
- 2. AI and Machine Learning for Predictive Analytics in Green Finance**
Track: "AI-driven Predictive Analytics"
Challenge: Create innovative AI and machine learning models that can predict trends and risks in green finance, helping financial institutions make informed and sustainable investment decisions.

Participants can use any datasets they prefer.
- 3. Behavioral Analytics for Detecting Anomalies in Financial Transactions**
Track: "Behavioral Analytics for Security"
Challenge: Implement and improve behavioral analytics solutions that can detect anomalies in financial transactions, providing enhanced security against fraudulent activities.

Participants can use any datasets they prefer.
- 4. Secure Cloud-Native Solutions for Financial Institutions**
Track: "Cloud-Native Security Frameworks"
Challenge: The team can work on developing secure cloud-native solutions tailored to the unique needs of financial institutions, ensuring data privacy and integrity in the cloud.

Participants have the flexibility to choose from various contemporary cloud-native challenges.



The screenshot shows a web browser window with a presentation slide and a sidebar.

Top Bar: Shows standard browser controls: back, forward, and refresh.

Title Bar: Shows the URL `docs.google.com`.

Left Sidebar:

- File Management: Includes icons for New File, Open, Save, and Recent files (29).
- Personal: Includes a Personal folder icon.
- Recent Items: Includes "gettin started with Groww", "IITK Hacks", "IITM Hacks", "Files to check", "temp spam", "Colorful Modern Business I...", "My Application - Realtime...", and "Vishwa-docs/IIT-Madras-E...".
- Search: A search bar with placeholder text "Search Google Drive".
- Bottom Buttons: Includes a "New Tab" button and a "+" button.

Right Content Area:

A presentation slide is displayed with the following content:

- Section 2:** Indicated by a blue triangle icon.
- Section Header:**

temenos
- Submission Format:**

Submissions will be accepted through a Google Form, which should include the following:

 - PPT
 - Link to the GitHub repository
 - Demo video
- Evaluation Framework:**

We expect a feasible and scalable solution for the given problem statements, a prototype or code implementation accompanied by

 - Documentation - Detailed Readme files with setup instructions, data resources used, Processing done on the data, model results, or output
 - Innovative features
 - Demo Video

Will provide you with a distinct advantage.