Projects (2018 – 2024):

(If the Github links run into error 404, it means the project is not open source and it is a private repository.)

(The projects start from 2018 and go forward chronologically. The older projects may seem stupid because I didn't know much back then.)

1. Phone Interface (2018): A Java based project to mimic the phone dialler. It showed a phone dialler GUI and calls made with that would be placed via a connected android phone over ADB. It could install ADB drivers for connected android devices, make and receive calls, send SMS, autonomously answer calls (and play a pre-recorded message.)
   https://github.com/AdityaMitra5102/PhoneInterface
2. Titrator (2018): An Arduino based project for electrochemistry-based acid-base titration. It consisted of a standard burette containing an acid and the base was provided in a beaker or a conical flask. Electrodes connected to the Arduino were introduced in the conical flask and the stopcock of the burette was controlled with a servo motor by the Arduino. The stopcock would be closed when the base was perfectly neutralized by the acid.
   https://github.com/AdityaMitra5102/Titrator
3. ADB Lock (2018): This is a file lock application that used the user's android device as an authentication tool. To open the file, the user had to connect his android phone over the USB cable to the computer. It checked the serial number of the device over ADB before unlocking the file.
   https://github.com/AdityaMitra5102/adbLock
4. Invisible Encryption (2019): A java-based implementation of a custom substitution cipher. It involved transposition using matrices and substituting each character with two non-graphic characters to make it unreadable by humans. This would be done multiple times to encrypt the text. The reverse would be applied to decrypt it.
   https://github.com/AdityaMitra5102/InvisibleEncryption
5. Desktop Handsfree (2019): This allowed you to turn on a computer from a phone over Bluetooth. It is different from Standard Wake-On-Lan procedures since it does not use the network. Wake-On-Lan devices need to be connected to the LAN over a wired connection and that is a limitation. Desktop Handsfree works by adding an Arduino based module inside the cabinet, connected directly to motherboard SW pins. When it receives the signal from phone over Bluetooth, it triggers a transistor to emulate the power button of the CPU being pressed.
   https://github.com/AdityaMitra5102/DesktopHandsfree
6. Chat Server CLI (2020): This is probably the beginning of me building Remote Access Trojans. It is a socket-based chat application based on Java. It had the added feature that when the server sends a CLI command, the client machine would execute it.
   https://github.com/AdityaMitra5102/ChatServerCLI
7. Flexi Luminos (2020): A Raspberry Pi based smart home automation. It allowed the user to control home devices like lights and fans over multiple channels like using QR Codes, using Alexa or Google Home, using a web interface, using an android app,

using discord and telegram bots, or via exposed APIs. It was built with Java and Python.
https://github.com/AdityaMitra5102/PaperSwitch

8. Defense Zoid (2020): A Raspberry Pi based smart lock for vaults and safe. It used similar logic as in ADB Lock to use the user's Android device as the authentication device. It used cloud-based remote device management.
https://github.com/AdityaMitra5102/Defensezoid
9. Tsuyoi (2020): A HC-05 Bluetooth module-based panic button key-chain for women safety. The main merit of this project is that it did not use any microcontroller like an Arduino nano. It consisted of the Bluetooth module connected to a battery and a button. Pressing the button would short the battery momentarily, thus disconnecting the module from the connected smartphone and this would be used as a panic signal. No-reliance on microcontroller allowed to boost the battery life. It had emergency contact and law-enforcement dashboard features.
https://github.com/AdityaMitra5102/DSCWOW-Tsuyoi
10. Adam's Ale (2021): It is an Arduino-based water quality testing kit. It is focused on the use-cases of quickly finding potable water in disaster zones. Any personnel could test the water quality of a source by simply dipping the probe and if the water was safe to drink it would be automatically updated to an online database. The disaster victims could access this database in a map-view if they had internet connectivity. For places where internet is disrupted, this could be accessed by SMS and the server would return the road directions to the water source via SMS.
https://github.com/AdityaMitra5102/Adams_Ale
https://www.sciencedirect.com/science/article/pii/S2667010022001731
11. Braille Cam (2021): It is a finger mounted camera that could help visually impaired persons read books. The finger mounted camera could be faced towards the book to be read and it would apply OCR to read the book via a headphone. It is based on Raspberry Pi. It further had the feature to capture pages of the book for future reference and it would be stored on cloud.
https://github.com/AdityaMitra5102/BrailleCam
12. Audio Drop (2021): An NFC based project for faster pairing of Bluetooth speakers. NFC stickers would be attached to the Bluetooth Speakers and tapping the phone on it would attempt to connect to the speaker. If the speaker is not paired, it would attempt to pair and connect the device.
https://github.com/AdityaMitra5102/ADrop
https://adityamitra5102.github.io/certs/IPR2021076_Published.pdf
13. Corazon Shirt (2021): A shirt with EEG probes and SpO2 sensor, connected via an Arduino. It would give real time health statistics and emergency alert in case of medical emergencies. It is ideal for gym goers and elderly people.
https://github.com/AdityaMitra5102/Corazon_Shirt
14. Mario Shooter (2021): It is a game made with Processing as a part of my Computer Graphics class course project. It is 2D shooting game.
https://github.com/AdityaMitra5102/Mario_Shooter
15. Loki (2022): It is a physical security lock based on FIDO2. It is a standard for smart Safes and Vaults so that it could be used with cryptographic authentication with Physical Security keys. It had cloud-based management portal where security keys

could be remotely assigned and removed in-case of damage or theft.
https://github.com/AdityaMitra5102/IoT-Physical-Security
https://ieeexplore.ieee.org/abstract/document/9927414

16. Safe Band (2022): An NFC Based Women safety band. The band is supposed to be a simple NFC tag without any electronic components. When tapped against anyone's smartphone, it would trigger an API Call, signifying the distress. It would be logged in a database; emergency contacts will be notified and would maintain a dashboard for law enforcement.
https://github.com/AdityaMitra5102/Safe-Band
17. Reverse Proxy (2022): It is a FIDO2 based easy attendance system for educational institutes as well as for enterprises. It involves displaying a dynamic QR code by a projector or any other means. It can be scanned by the students and it would prompt them for their fingerprint or device lock of their smartphones. It uses the principles of cryptographic authentication to ensure attendance process is seamless and the overall attendance process would take only one tap on the user's smartphone, so it is very seamless.
https://github.com/AdityaMitra5102/Reverse_Proxy
18. Terminal Bot (2022): It is a Remote Access Trojan (Malware) weaponized using HID Injection using a Raspberry Pi Pico. When the Pico is plugged into the victim's computer, it downloads and installs the malware, giving the C2 to the attacker over a telegram bot.
https://github.com/AdityaMitra5102/TerminalBot
19. Missile Detonator (2022): A completely offline and airgapped two-crew system to trigger a relay. The two-crew system used FIDO2 compatible physical security keys over wired connectivity to a RPi Based controller connected to a relay. This is inspired from two crew systems for Torpedoes and Missiles. It could be used offline in any critical system and the Relay could be used to trigger weapon systems.
https://github.com/AdityaMitra5102/missile-detonation
20. MAuthN (2022): It is a passwordless authentication solution for all devices, including IoT, Wearables and more without enough compute resources. It leveraged a smartphone app to transfer the authentication. It employs multi-factor cryptographic and biometric authentication to ensure strong identity verification. It is a robust system and ensure all logs are maintained. It gives easy SDK and APIs for implementation on various platforms.
https://github.com/AdityaMitra5102/MAuthN-Backend
https://github.com/AdityaMitra5102/MAuthN-SDK
https://github.com/AdityaMitra5102/Mauthn-App
21. Medical Record Management System (2023): A FIDO2 based patient-centric medical records management system. It made the patient in control of their Electronic Health Records (EHR) and gave them the provision to temporarily allow hospitals and medical institutions to access their data. It further exposed an API for medical devices to be able to directly upload the reports after medical tests.
https://github.com/AdityaMitra5102/Medical-Record
https://www.inderscienceonline.com/doi/abs/10.1504/IJCCBS.2024.139105
22. Seamless payments framework (2023): A FIDO2 based financial transaction system. It needed authentication to both receive and send money, this mitigating multiple

financial scams. Further, it involved tokenizing money in the form of as-good-as-cash NFC tokens. The tokens could be redeemed to get the money in the account.
https://github.com/AdityaMitra5102/FIDO-Payments
https://arxiv.org/abs/2408.04977

23. Anti-screen capture (2023): Built as a part of my Computer Vision class coursework, this project mitigated the risk if taking a picture of the screen containing sensitive content with external devices like a phone or camera. It used webcam feed to identify whether a phone or camera is attempting to take a picture of the screen and minimizing all open windows in that case.
https://github.com/AdityaMitra5102/Anti-Screencapture-With-Phone
24. Connet (2023): It is a rapid network identity changer for anonymity in the local network and internet. It is a java-based application that repeatedly changes the MAC address, IP address and uses VPN to make the user completely anonymous in local network as well as on the internet. It works on Linux based devices.
https://github.com/AdityaMitra5102/Connet
25. TutorGPT (2023): A simple RAG deployed on a web-based framework. It let the users upload their study materials in various formats including PDFs and then query the same using a LLM.
https://github.com/AdityaMitra5102/TutorGPT
26. Password Exfiltration (2023): It is a RPi Pico based HID Injection attack. When the Pico is connected to the victim's machine, it would exfiltrate all saved WIFI networks and their passwords and send it to the attacker using a telegram bot.
https://github.com/AdityaMitra5102/PasswodExfiltratorPico
27. TUSH-Key (2023): Transferrable User Secrets on Hardware Key. It is a framework for handling multiple FIDO2 authenticators for a particular service. The framework enabled creating multiple public key keypairs on the authenticators instead of syncing secrets, thus making it more secure than passkeys.
https://github.com/AdityaMitra5102/Tushkey
https://arxiv.org/abs/2307.07484
28. MetaKey (2023): A Metaverse platform that used handsfree authentication with MAuthN. It mitigated risks of identity thefts and fake accounts in metaverse platforms. It was implemented on a fork of BabylonJS.
https://github.com/AdityaMitra5102/Metaverse
https://ieeexplore.ieee.org/abstract/document/10026952
https://arxiv.org/abs/2301.01770
29. MERP (2023): Metaverse Extended Reality Portal. It is an Arduino-based wearable jacket that had sensors and a shoulder mounted projector. It could translate the user's movements into a metaverse environment and show the environment in front of him, in first person view using the projector.
https://github.com/AdityaMitra5102/metarealityportal
https://arxiv.org/abs/2402.05592
30. Saila (2023): A HID Injection attack mitigation service, built on top of MAuthN. It blocked all newly connected HID Devices unless explicitly authenticated using the MAuthN mobile app. It ensured even if the attacker had physical access to the target's computer, he wouldn't be able to plug in a rubber ducky.

https://github.com/AdityaMitra5102/MAuthN-Rubber-ducky-protection
https://ieeexplore.ieee.org/abstract/document/10660705

31. Cinnamon FIDO Plugin (2024): A plugin that added FIDO2 based passwordless authentication support to the lock screen of Cinnamon Desktop Environment in Linux.
https://github.com/AdityaMitra5102/Cinnamon-FIDO-Plugin
32. Entra ID Console (2024): A framework that allowed passwordless authentication of delegated access to Azure Entra ID directly from any application, including console applications without using the web browser.
https://github.com/AdityaMitra5102/Entra-ID-console
33. One Bit Boolean (2024): It is a data structure based on java that reserved only 1 bit for storing a Boolean variable. This is opposed to the general primitive variable that reserves a whole byte to store a Boolean.
https://github.com/AdityaMitra5102/OneBitBoolean
34. Pocket ID (2024): It is a Raspberry Pi Zero W based device that connects to the local network and manages all passwordless authentication. It's like a physical cryptographic hardware that resides on the network and can be used with multiple devices together. It has been tested with multiple authentication platforms, including the Google SSO.
https://github.com/AdityaMitra5102/PocketID
35. NetLM (2024): It is a Cisco iOS devices configuration framework based on Llama 3. It allows the user to specify the desired configuration or the goals in plain English and the system will generate the commands to do that using Llama and apply the configurations to the Cisco device over SSH, Telnet or Serial.
https://github.com/AdityaMitra5102/NetLM
36. Colaboot (2024): This is a framework to batch configure operating systems for multiple computers using an IPython notebook (like Google Colab) and then be able to instantly boot the computers using the configured OS. The computers may not have any disk or persistent storage and it would work mostly on network boot. This mitigates multiple attack vectors used by Advanced persistent threats (APTs).
https://github.com/AdityaMitra5102/Colab-boot
https://arxiv.org/abs/2408.17045
37. BSOD As a Service (2024): This is not a big project, but just something built for a prank. It allows you to crash any Windows PC on the network with a Blue Screen of Death by triggering a kernel bug check remotely.
https://github.com/AdityaMitra5102/BSOD-as-a-Service
38. Post Quantum Passwordless (2024): Probably the world's first implementation of Passwordless authentication based on Post Quantum cryptography using the Crystals-Dilithium standard (FIPS 204). It demonstrates a web-based backend and a daemon and web extension to enable Post Quantum passwordless on a standard web browser.
https://github.com/AdityaMitra5102/Post-Quantum-Passwordless
39. QNet (2024): A remote terminal access platform (like SSH or Telnet) but it is encrypted with Post Quantum Cryptography. Crystals-Kyber algorithm is used to implement QNet.
https://github.com/AdityaMitra5102/QNet

40. BIDO (2024): Biometric Identity Online. It is a proposed standard that involves using the cryptographic hash of facial features of a user to generate ECDSA keypair. This keypair is then used to perform cryptographic authentication. Here, the facial features and secrets are not stored anywhere, making the face the only authentication key. https://github.com/AdityaMitra5102/BIDO
41. Zero Frontend (2024): It is a proof of concept to show how easily websites can be built using LLMs. It is a JavaScript based framework that can build and deploy an entire website with a single prompt. https://github.com/AdityaMitra5102/ZeroFrontend
42. Force RSA on FIDO (2024): This is a web extension that forces the use of only RSA on FIDO2 authentication. This is inspired from a rumour that ECDSA using the NIST P-256 curve might be backdoored and RSA would be a safer alternative for authentication. https://github.com/AdityaMitra5102/ForceRSAonFIDO
43. Ubuntu in TWRP (2024): It allows you to dual boot a rooted android device to Ubuntu. It uses the TWRP (Team Win Recovery Project) to start Ubuntu while in recovery mode. https://github.com/AdityaMitra5102/ubuntu-in-TWRP
44. AirCopy (2024): It allows you to share file from one PC to another with hand gesture. It involves advanced networking to determine and the sender and receiver of the files, perform a handshake and do a zero-touch file share. https://github.com/AdityaMitra5102/AirCopy